



**TUGAS AKHIR - KI141502**

# **PENGUJIAN KERAHASIAAN DATA DAN OTENTISITAS PENGGUNA PADA SISTEM E-PKK ONLINE MENGGUNAKAN ISO 25010**

**ARANDA RIZKI SOEDJONO**  
**NRP 5112 100 068**

**Dosen Pembimbing**  
**Dr. Ir. Siti Rochimah, M.T.**  
**Ratih Nur Esti Anggraini, S.Kom., M.Sc.**

**JURUSAN TEKNIK INFORMATIKA**  
**Fakultas Teknologi Informasi**  
**Institut Teknologi Sepuluh Nopember**  
**Surabaya 2016**

*[Halaman ini sengaja dikosongkan]*



**FINAL PROJECT - KI141502**

# **CONFIDENTIALITY AND AUTHENTICITY TESTING FOR ONLINE E-PKK SYSTEM USING ISO 25010**

**ARANDA RIZKI SOEDJONO**  
**NRP 5112 100 068**

Advisor  
Dr. Ir. Siti Rochimah, M.T.  
Ratih Nur Esti Anggraini, S.Kom., M.Sc.

**INFORMATICS DEPARTMENT**  
Faculty of Information Technology  
Institut Teknologi Sepuluh Nopember  
Surabaya 2016

*[Halaman ini sengaja dikosongkan]*

**PENGUJIAN KERAHASIAAN DATA DAN OTENTISITAS  
PENGUNA PADA SISTEM E-PKK ONLINE  
MENGUNAKAN ISO 25010**

**TUGAS AKHIR**

Diajukan Guna Memenuhi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer  
pada  
Rumpun Mata Kuliah Rekayasa Perangkat Lunak  
Program Studi S-1 Jurusan Teknik Informatika  
Fakultas Teknologi Informasi  
Institut Teknologi Sepuluh Nopember

Oleh :  
**ARANDA RIZKI SOEDJONO**  
NRP : 5112 100 068

Disetujui oleh Dosen Pembimbing Tugas Akhir :

Dr. Ir. Siti Rochimah, M.T.

NIP: 196810021994032001

Ratih Nur Esti Anggraini, S.T., M.Sc.

NIP: 198412102014042003



**SURABAYA  
JUNI 2016**

*[Halaman ini sengaja dikosongkan]*

**PENGUJIAN KERAHASIAAN DATA DAN OTENTISITAS  
PENGGUNA PADA SISTEM E-PKK ONLINE MENGGUNAKAN  
ISO 25010**

Nama Mahasiswa : ARANDA RIZKI SOEDJONO  
NRP : 5112 100 068  
Jurusan : Teknik Informatika ITS  
Dosen Pembimbing I : Dr. Ir. Siti Rochimah, M.T.  
Dosen Pembimbing II : Ratih Nur Esti Anggraini, S.Kom., M.Sc.

**Abstrak**

*Sistem e-PKK online merupakan sebuah sistem informasi manajemen untuk komunitas PKK dan Posyandu. Sistem tersebut terdiri dari dua buah sub-sistem untuk menangani kebutuhan komunitas PKK dan Posyandu, masing-masing terdiri dari aplikasi web dan aplikasi perangkat bergerak, serta sebuah aplikasi perangkat bergerak ensiklopedia seputar kesehatan balita dan ibu hamil. Namun beberapa fitur yang disediakan sistem belum menjamin adanya keamanan informasi yang disimpan dan dimiliki oleh pengguna tertentu. Selain itu, sistem ini masih belum dapat mengenali pengguna yang masuk ke dalamnya sehingga tidak ada penyaringan informasi saat seorang pengguna menggunakan sistem. Oleh karena itu, sistem akan diuji menggunakan standar penjaminan kualitas perangkat lunak yang sudah ada agar informasi pribadi seorang pengguna dapat dengan aman disimpan di dalam sistem dan hanya dapat diakses oleh pihak yang memiliki.*

*Pengujian kualitas perangkat lunak menggunakan standar ISO 25010 yang menaungi karakteristik-karakteristik standar penjaminan kualitas perangkat lunak. Karakteristik kualitas perangkat lunak yang akan diujikan pada Tugas Akhir ini adalah kerahasiaan data dan otentisitas pengguna, yang merupakan sub-karakteristik dari karakteristik keamanan pada ISO 25010. Pemilihan karakteristik tersebut didasari kebutuhan sistem akan kesesuaian informasi yang dapat diterima oleh pengguna tertentu dan kebutuhan sistem akan terjaminnya keamanan informasi*

*penting pengguna yang dipertukarkan antar aplikasi di dalamnya. Pengujian dilakukan dengan menghitung metrik yang telah disediakan pada standar ISO. Apabila hasil perhitungan dinilai kurang memuaskan maka akan diaplikasikan pembenaran pada sistem agar memenuhi metrik tersebut.*

***Kata kunci: sistem, online, kualitas, pengujian, kerahasiaan, otentisitas, ISO 25010, metrik.***



## **CONFIDENTIALITY AND AUTHENTICITY TESTING FOR ONLINE E-PKK SYSTEM USING ISO 25010**

Name : ARANDA RIZKI SOEDJONO  
NRP : 5112 100 068  
Major : Informatics Department – ITS  
Supervisor I : Dr. Ir. Siti Rochimah, M.T.  
Supervisor II : Ratih Nur Esti Anggraini, S.Kom., M.Sc.

### **Abstract**

*Online e-PKK system is a management information system for PKK and Posyandu community. This system consists of two subsystems to handle PKK and Posyandu community needs, each will consists of web application and mobile application, and a mobile encyclopedia application about toddler and pregnant mother health. However, some features provided by the system not yet ensure the confidentiality of information saved in it and owned by certain user. Moreover, this system has not yet recognized user logging inside it, so that there is no information filtering when a user using the system. Therefore, system will be tested based on existing software quality assurance standard so that personal user information will be safely kept in the system and can be accessed only by the owner.*

*Software quality testing will be using ISO 25010 standard which covers software quality assurance standard characteristics. Software quality characteristics which will be tested in this final project are confidentiality and authenticity, which are sub-characteristics of security characteristic in ISO 25010. These characteristics were picked based on system need about information conformity received by certain user and system need about important confidentiality assurance on important user information traded inter-application inside it. Testing will be done by measuring provided metrics by ISO standard. If the result is judged not yet satisfying then some fixes will be applied on the system to satisfy the certain metric.*

***Kwywords: system, online, quality, testing, confidentiality, authenticity, ISO 25010, metrics.***

## KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Segala puji dan syukur ke hadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul ***“Pengujian Kerahasiaan Data dan Otentisitas Pengguna pada Sistem E-PKK Online Menggunakan ISO 25010”***.

Dalam pelaksanaan Tugas Akhir ini tentu penulis sebagai makhluk sosial tidak dapat menyelesaikannya tanpa bantuan dari pihak lain. Tanpa mengurangi rasa hormat, penulis memberikan penghargaan serta ucapan terima kasih yang sebesar-besarnya kepada:

1. Orang tua, saudara, serta keluarga besar yang senantiasa memberikan semangat dan doa agar penulis dapat menyelesaikan Tugas Akhir dengan tepat waktu.
2. Ibu Dr. Ir. Siti Rochimah, M.T. selaku dosen pembimbing Tugas Akhir pertama yang telah membimbing, memotivasi, dan memberikan banyak masukan dalam pengerjaan Tugas Akhir ini.
3. Ibu Ratih Nur Esti Anggraini, S.Kom., M.Sc. selaku dosen pembimbing Tugas Akhir kedua yang selalu memberikan koreksi serta masukan-masukan yang dapat penulis kembangkan dari Tugas Akhir ini.
4. Bapak dan Ibu dosen Jurusan Teknik Informatika ITS yang telah mengajarkan banyak ilmu berharga kepada penulis.
5. Bapak dan Ibu karyawan Jurusan Teknik Informatika ITS atas berbagai bantuan yang telah diberikan kepada penulis selama masa perkuliahan.
6. Teman-teman mahasiswa bidang minat Rekayasa Perangkat Lunak yang telah menemani perjuangan mencari ilmu selama mengambil mata kuliah RMK RPL.

7. Teman-teman administrator Laboratorium RPL yang selalu setia menemani hari-hari saya.
8. Teman-teman dari UKM PSM ITS dan LMB ITS yang telah mengisi hari-hari penulis selain wajib perkuliahan namun tetap aktif di organisasi kemahasiswaan dan minat bakat.
9. Teman-teman Teknik Informatika ITS angkatan 2012, yang telah memberikan warna-warni kehidupan mahasiswa mulai sejak mahasiswa baru hingga lulus.
10. Pihak-pihak lain yang tidak sempat penulis sebutkan, yang telah membantu kelancaran pengerjaan Tugas Akhir ini.

Penulis sangat berharap bahwa apa yang dihasilkan dari tugas akhir ini bisa memberikan manfaat bagi semua pihak, khususnya bagi diri penulis sendiri dan seluruh *civitas academica* Teknik Informatika ITS, serta bagi agama, bangsa, dan negara. Tak ada manusia yang sempurna sekalipun penulis berusaha sebaik mungkin dalam menyelesaikan Tugas Akhir ini. Karena itu, penulis memohon maaf apabila terdapat kesalahan, kekurangan, maupun kelalaian yang telah penulis lakukan. Kritik dan saran yang membangun sangat diharapkan oleh penulis untuk dapat disampaikan untuk perbaikan selanjutnya.

Surabaya, Juni 2016

Aranda Rizki Soedjono

## DAFTAR ISI

<b>Abstrak .....</b>	<b>ix</b>
<b>Abstract .....</b>	<b>xi</b>
<b>KATA PENGANTAR.....</b>	<b>xiii</b>
<b>DAFTAR ISI .....</b>	<b>xv</b>
<b>DAFTAR GAMBAR.....</b>	<b>xix</b>
<b>DAFTAR TABEL .....</b>	<b>xxi</b>
<b>DAFTAR KODE SUMBER .....</b>	<b>xxv</b>
<b>1 BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	5
1.3. Batasan Masalah .....	6
1.4. Tujuan .....	6
1.5. Metodologi.....	7
1.6. Sistematika Penulisan.....	11
<b>2 BAB II TINJAUAN PUSTAKA.....</b>	<b>13</b>
2.1. Sistem e-PKK <i>Online</i> .....	13
2.2. ISO 25010 .....	14
2.3. Kerahasiaan Data ( <i>Confidentiality</i> ) .....	15
2.4. Otentisitas Pengguna ( <i>Authenticity</i> ) .....	17
2.5. Kerangka Kerja <i>Laravel</i> .....	18
2.6. Kerangka Kerja <i>PhoneGap</i> .....	18
<b>3 BAB III ANALISIS DAN PERANCANGAN .....</b>	<b>19</b>
3.1. Analisis Sistem e-PKK <i>Online</i> .....	19

3.1.1.	Kerahasiaan Data Sistem .....	20
3.1.2.	Otentistias Pengguna Sistem.....	21
3.2.	Perancangan Pengujian ISO 25010.....	22
3.3.	Perancangan Manajemen Kerahasiaan Data .....	26
3.4.	Perancangan Manajemen Otentisitas Pengguna.....	30
3.5.	Perancangan Fitur Mengenai Kerahasiaan Data dan Otentisitas Pengguna .....	31
3.5.1.	Rancangan Kebutuhan Fungsionalitas .....	32
3.5.2.	Rancangan Kasus Penggunaan Tambahan Sistem 40	
3.5.3.	Rancangan Basis Data .....	54
3.6.	Perancangan Antarmuka Pengguna .....	58
3.6.1.	Rancangan Antarmuka Halaman Login .....	58
3.6.2.	Rancangan Antarmuka Halaman Verifikasi Akun 59	
3.6.3.	Rancangan Antarmuka Halaman Lihat Profil Akun 61	
<b>4</b>	<b>BAB IV IMPLEMENTASI.....</b>	<b>63</b>
4.1.	Lingkungan Implementasi .....	63
4.2.	Implementasi Proses .....	63
4.2.1.	Implementasi Konfigurasi Otentikasi <i>Laravel 5.1</i> 63	
4.2.2.	Implementasi Perangkat Tengah ( <i>Middleware</i> ) ..	66
4.2.3.	Implementasi Pengolahan Kata Sandi Akun Perangkat Bergerak .....	67
4.2.4.	Implementasi Algoritma Mendapatkan Token....	69

4.2.5.	Implementasi Pengecekan Konfirmasi Token Akun	70
4.3.	Implementasi Antarmuka Pengguna.....	72
4.3.1.	Halaman Login.....	72
4.3.2.	Halaman Verifikasi Akun Perangkat Bergerak...	72
4.3.3.	Halaman Profil Akun .....	73
<b>5</b>	<b>BAB V UJI COBA DAN EVALUASI.....</b>	<b>77</b>
5.1.	Lingkungan Uji Coba.....	77
5.2.	Skenario Uji Coba.....	77
5.2.1.	Pengujian Fungsionalitas.....	78
5.2.2.	Pengujian Kerahasiaan Data dan Otentisitas Pengguna Menggunakan ISO 25010.....	87
5.3.	Evaluasi.....	105
5.3.1.	Evaluasi Pengujian Fungsionalitas .....	105
5.3.2.	Evaluasi Pengujian Kerahasiaan Data dan Otentisitas Pengguna Menggunakan ISO 25010 .....	105
<b>6</b>	<b>BAB VI KESIMPULAN DAN SARAN.....</b>	<b>109</b>
6.1.	Kesimpulan .....	109
6.2.	Saran .....	110
	<b>DAFTAR PUSTAKA.....</b>	<b>111</b>
<b>7</b>	<b>LAMPIRAN A.1. Kebutuhan Sistem PKK <i>Online</i> .....</b>	<b>113</b>
<b>8</b>	<b>LAMPIRAN A.2. Basis Data Sistem e-PKK <i>Online</i> .....</b>	<b>137</b>
	<b>BIODATA PENULIS .....</b>	<b>139</b>

*[Halaman ini sengaja dikosongkan]*



## DAFTAR GAMBAR

Gambar 1.1. Gambaran keseluruhan sistem e-PKK <i>online</i> .....	2
Gambar 2.1. Model Kualitas Perangkat Lunak ISO 25010 .....	15
Gambar 3.1. Diagram Alir Pengujian ISO 25010 .....	22
Gambar 3.2. Penyesuaian Kasus Penggunaan "Mengolah data PKK" .....	28
Gambar 3.3. Perancangan kerahasiaan data menggunakan <i>middleware</i> .....	29
Gambar 3.4. Proses registrasi pengguna perangkat bergerak baru .....	31
Gambar 3.5. Proses apabila pengguna kehilangan token.....	32
Gambar 3.6. Proses verifikasi pengguna perangkat bergerak .....	32
Gambar 3.7. Kasus Penggunaan Tambahan Sistem .....	40
Gambar 3.8. Diagram Aktivitas: Melihat Profil Akun .....	46
Gambar 3.9. Diagram Aktivitas: Ubah Nama Pengguna .....	48
Gambar 3.10. Diagram Aktivitas: Ubah Kata Sandi .....	49
Gambar 3.11. Diagram Aktivitas: <i>Reset</i> Token Akun .....	51
Gambar 3.12. Diagram Aktivitas: Verifikasi Akun .....	52
Gambar 3.13. Diagram Aktivitas: Mengelola Akun Pengguna .....	54
Gambar 3.14. PDM Perubahan Sistem PKK .....	55
Gambar 3.15. PDM Perubahan Sistem Posyandu .....	56
Gambar 3.16. PDM bagian penghubung (manajemen pengguna) sistem e-PKK <i>online</i> .....	57
Gambar 3.17. PDM bagian penghubung (lokasi) sistem e-PKK <i>online</i> .....	57
Gambar 3.18. Rancangan Antarmuka Halaman Login .....	58
Gambar 3.19. Rancangan Antarmuka Halaman Verifikasi Akun Perangkat Bergerak.....	59
Gambar 3.20. Rancangan Antarmuka Halaman Profil Akun .....	60
Gambar 4.1. Implementasi Antarmuka Halaman Login .....	73
Gambar 4.2. Implementasi Antarmuka Halaman Verifikasi Akun Perangkat Bergerak.....	74
Gambar 4.3. Rancangan Antarmuka Halaman Profil Akun .....	75
Gambar 5.1. Pengujian Fitur Melihat Profil Akun .....	79

Gambar 5.2. Pengujian Fitur Mengubah Nama Pengguna Skenario 1 .....	80
Gambar 5.3. Pengujian Fitur Mengubah Nama Pengguna Skenario 2 .....	82
Gambar 5.4. Pengujian Fitur Mengubah Kata Sandi Skenario 1 .....	83
Gambar 5.5. Pengujian Fitur Mengubah Kata Sandi Skenario 2 .....	83
Gambar 5.6. Pengujian Fitur <i>Reset</i> Token Akun .....	84
Gambar 5.7. Pengujian Fitur Verifikasi Akun .....	85
Gambar 5.8. Pengujian Fitur Mengelola Akun Pengguna .....	86
Gambar 8.1. Diagram Kasus Penggunaan Aplikasi Web PKK.....	115
Gambar 8.2. Diagram Aktivitas: Mengelola Data PKK.....	119
Gambar 8.3. Diagram Aktivitas: Mengelola Periode Kepengurusan .....	120
Gambar 8.4. Diagram Aktivitas: Mengelola Jabatan Pengurus .....	121
Gambar 8.5. Diagram Aktivitas: Mengelola Pengurus PKK ....	122
Gambar 8.6. Diagram Aktivitas: Mengelola Anggota PKK .....	124
Gambar 8.7. Diagram Aktivitas: Mengelola Kas PKK .....	125
Gambar 8.8. Diagram Aktivitas: Mengelola Jenis Kas PKK ....	126
Gambar 8.9. Diagram Aktivitas: Mengelola Absen.....	127
Gambar 8.10. Diagram Aktivitas: Mengelola Notulensi.....	128
Gambar 8.11. Diagram Aktivitas: Mengelola Pengumuman ....	130
Gambar 8.12. Diagram Aktivitas: Mengelola Laporan Bidang .....	131
Gambar 8.13. Diagram Aktivitas: Mengelola Data Jentik Nyamuk .....	132
Gambar 8.14. Diagram Aktivitas: Menampilkan Daftar Keluhan .....	133
Gambar 8.15. Diagram Aktivitas: Mengirimkan Komentar Baru .....	134
Gambar 9.1. PDM Sistem Posyandu .....	137
Gambar 9.2. PDM Sistem PKK.....	138

## DAFTAR TABEL

Tabel 3.1. Contoh Perhitungan Metrik Kemampuan Pengendalian Akses .....	23
Tabel 3.2. Contoh Perhitungan Metrik Ketepatan Enkripsi Data.....	24
Tabel 3.3. Contoh Perhitungan Metrik Kekuatan Kriptografi Algoritma.....	24
Tabel 3.4. Contoh Perhitungan Metrik Kesesuaian Protokol Otentikasi.....	25
Tabel 3.5. Contoh Perhitungan Metrik Kesesuaian Aturan Otentikasi.....	26
Tabel 3.6. Petunjuk Penulisan Perbandingan Sistem.....	33
Tabel 3.7. Daftar Perbandingan Kebutuhan Fungsionalitas .....	34
Tabel 3.8. Daftar Perbandingan Deskripsi Diagram Kasus Penggunaan.....	41
Tabel 3.9. Spesifikasi Kasus Penggunaan: Melihat Profil Akun .....	46
Tabel 3.10. Spesifikasi Kasus Penggunaan: Ubah Nama Pengguna .....	47
Tabel 3.11. Spesifikasi Kasus Penggunaan: Ubah Kata Sandi ...	50
Tabel 3.12. Spesifikasi Kasus Penggunaan: <i>Reset</i> Token Akun. ....	50
Tabel 3.13. Spesifikasi Kasus Penggunaan: Verifikasi Akun.....	52
Tabel 3.14. Spesifikasi Kasus Penggunaan: Mengelola Akun Pengguna .....	53
Tabel 4.1. Lingkungan Implementasi Sistem .....	63
Tabel 4.2. Daftar Implementasi Perangkat Tengah .....	66
Tabel 5.1. Lingkungan Uji Coba Aplikasi Web ( <i>laptop</i> ) .....	77
Tabel 5.2. Lingkungan Uji Coba Aplikasi Perangkat Bergerak ( <i>smartphone</i> ).....	77
Tabel 5.3. Pengujian Fitur Melihat Profil Akun .....	78
Tabel 5.4. Pengujian Fitur Mengubah Nama Pengguna Skenario 1 .....	81
Tabel 5.5. Pengujian Fitur Mengubah Nama Pengguna Skenario 2 .....	81
Tabel 5.6. Pengujian Fitur Mengubah Kata Sandi Skenario 1 ....	82
Tabel 5.7. Pengujian Fitur Mengubah Kata Sandi Skenario 2....	83

Tabel 5.8. Pengujian Fitur <i>Reset</i> Token Akun .....	84
Tabel 5.9. Pengujian Fitur Verifikasi Akun .....	85
Tabel 5.10. Pengujian Fitur Mengelola Akun Pengguna .....	86
Tabel 5.11. Deskripsi Aturan Penulisan Tabel Pengujian .....	87
Tabel 5.12. Pengujian Tahap Pertama (Kemampuan Pengendalian Akses) .....	88
Tabel 5.13. Pengujian Tahap Pertama (Ketepatan Enkripsi Data) .....	93
Tabel 5.14. Pengujian Tahap Pertama (Kekuatan Kriptografi Algoritma) .....	94
Tabel 5.15. Pengujian Tahap Pertama (Kesesuaian Protokol Otentikasi) .....	94
Tabel 5.16. Pengujian Tahap Pertama (Kesesuaian Aturan Otentikasi) .....	95
Tabel 5.17. Pengujian Tahap Kedua (Kemampuan Pengendalian Akses) .....	96
Tabel 5.18. Pengujian Tahap Kedua (Ketepatan Enkripsi Data) .....	101
Tabel 5.19. Pengujian Tahap Kedua (Kekuatan Kriptografi Algoritma) .....	102
Tabel 5.20. Pengujian Tahap Kedua (Kesesuaian Protokol Otentikasi) .....	103
Tabel 5.21. Pengujian Tahap Kedua (Kesesuaian Aturan Otentikasi) .....	104
Tabel 5.22. Rangkuman Hasil Pengujian Fungsionalitas .....	105
Tabel 5.23. Rangkuman Hasil Pengujian ISO 25010 .....	105
Tabel 5.24. Ringkasan Modifikasi Sistem e-PKK <i>Online</i> .....	107
Tabel 5.25. Daftar Peran Pengguna Sistem e-PKK <i>Online</i> .....	107
Tabel 8.1. Kebutuhan Fungsional Aplikasi Web PKK .....	113
Tabel 8.2. Deskripsi Diagram Kasus Penggunaan Aplikasi Web PKK .....	116
Tabel 8.3. Spesifikasi Kasus Penggunaan: Mengelola Data PKK .....	118
Tabel 8.4. Spesifikasi Kasus Penggunaan: Mengelola Periode Kepengurusan .....	119

Tabel 8.5. Spesifikasi Kasus Penggunaan: Mengelola Jabatan Pengurus .....	121
Tabel 8.6. Spesifikasi Kasus Penggunaan: Mengelola Pengurus PKK.....	122
Tabel 8.7. Spesifikasi Kasus Penggunaan: Mengelola Anggota PKK.....	123
Tabel 8.8. Spesifikasi Kasus Penggunaan: Mengelola Kas PKK .....	124
Tabel 8.9. Spesifikasi Kasus Penggunaan: Mengelola Jenis Kas PKK.....	125
Tabel 8.10. Spesifikasi Kasus Penggunaan: Mengelola Absen	127
Tabel 8.11. Spesifikasi Kasus Penggunaan: Mengelola Notulensi .....	128
Tabel 8.12. Spesifikasi Kasus Penggunaan: Mengelola Pengumuman .....	129
Tabel 8.13. Spesifikasi Kasus Penggunaan: Mengelola Laporan Bidang .....	130
Tabel 8.14. Spesifikasi Kasus Penggunaan: Mengelola Data Jentik Nyamuk .....	131
Tabel 8.15. Spesifikasi Kasus Penggunaan: Menampilkan Daftar Keluhan.....	133
Tabel 8.16. Spesifikasi Kasus Penggunaan: Mengirimkan Komentar Baru .....	134
Tabel 8.17. Fitur Aplikasi Ensiklopedia Kesehatan Balita dan Ibu Hamil .....	135
Tabel 8.18. Kebutuhan Non-Fungsional Sistem e-PKK <i>Online</i>	135

*[Halaman ini sengaja dikosongkan]*

## DAFTAR KODE SUMBER

Kode Sumber 4.1. Konfigurasi Otentikasi <i>Laravel</i> pada dokumen <i>app/User.php</i> .....	64
Kode Sumber 4.2. Konfigurasi Otentikasi <i>Laravel</i> pada dokumen <i>config/auth.php</i> .....	65
Kode Sumber 4.3. Konfigurasi Otentikasi <i>Laravel</i> pada dokumen <i>database/migrations/2016_03_26_172319_create_general_tables.php</i> .....	65
Kode Sumber 4.4. Implementasi Enkripsi AES <i>CryptoJS</i> pada Penyimpanan Kata Sandi Akun Perangkat Bergerak .....	68
Kode Sumber 4.5. Implementasi Dekripsi AES <i>CryptoJS</i> pada Proses <i>Login</i> Aplikasi Perangkat Bergerak .....	69
Kode Sumber 4.6. Implementasi Algoritma Mendapatkan Token .....	70
Kode Sumber 4.7. Implementasi Proses Pengecekan Konfirmasi Token Pengguna Perangkat Bergerak .....	71
Kode Sumber 4.8. Implementasi Pemeriksaan Kesesuaian Token pada <i>Server</i> .....	72

*[Halaman ini sengaja dikosongkan]*



# **BAB I**

## **PENDAHULUAN**

Bab ini membahas garis besar penyusunan Tugas Akhir yang meliputi latar belakang, rumusan dan batasan masalah, tujuan pembuatan, metodologi penyusunan Tugas Akhir, dan sistematika penulisan. Pemaparan bahasan dijelaskan pada subbab-subbab berikut.

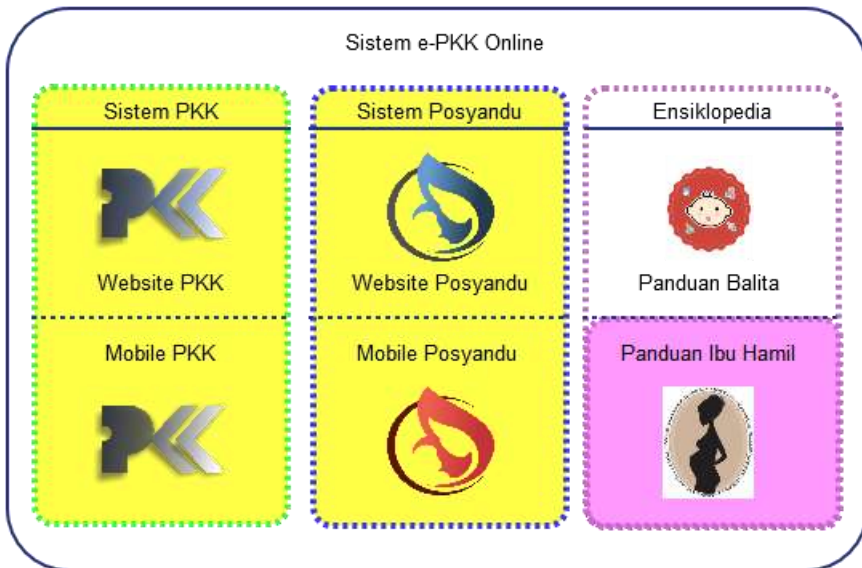
### **1.1. Latar Belakang**

Sistem e-PKK *online* merupakan sebuah sistem berskala nasional untuk menangani manajemen kegiatan dan komunitas yang dimotori oleh para wanita Indonesia, yakni PKK dan Posyandu. Kedua komunitas tersebut tersebar luas di seluruh Indonesia mulai dari tingkat nasional hingga tingkat Rukun Tetangga (RT). Aktivitas yang dilakukan oleh kedua komunitas tersebut berkaitan dengan administrasi kependudukan dan pembangunan pada suatu daerah yang dinaungi. Administrasi kependudukan dan pembangunan merupakan informasi yang sangat penting bagi negara sehingga perlu adanya suatu sistem untuk menangani manajemen informasi tersebut, tetapi tetap mudah dan nyaman untuk digunakan agar perkembangan dapat terus berjalan.

PKK, sebutan resmi dari gerakan Pemberdayaan dan Kesejahteraan Keluarga, adalah gerakan nasional dalam pembangunan masyarakat yang tumbuh dari bawah yang pengelolaannya dari, oleh, dan untuk masyarakat menuju terwujudnya keluarga yang beriman dan bertaqwa kepada Tuhan YME, berakhlak mulia dan berbudi luhur, sehat sejahtera, maju dan mandiri, kesetaraan dan keadilan *gender*, serta kesadaran hukum dan lingkungan [1]. Komunitas PKK merupakan sebuah organisasi yang dimotori oleh wanita-wanita pada suatu daerah. Tujuan dari komunitas PKK adalah membantu meningkatkan dan mewujudkan tertib administrasi kependudukan melalui pemberian

wawasan dan pengadaan kegiatan PKK yang berdasar pada 10 program pokok PKK [2].

Posyandu, kependekan dari Pos Pelayanan Terpadu, adalah salah satu bentuk upaya kesehatan bersumber daya masyarakat yang dikelola dan diselenggarakan dari, oleh, untuk, dan bersama masyarakat dalam penyelenggaraan pembangunan kesehatan, guna memberdayakan masyarakat dan memberikan kemudahan kepada masyarakat dalam memperoleh pelayanan kesehatan dasar untuk mempercepat penurunan angka kematian ibu dan bayi [3]. Aktivitas Posyandu didasari pada tujuh kegiatan Posyandu (Sapta Krida Posyandu), yakni kesehatan ibu dan anak, keluarga berencana, imunisasi, peningkatan gizi, penanggulangan diare, sanitasi dasar, dan penyediaan obat esensial [4]. Secara umum rutinitas Posyandu adalah pemeliharaan kesehatan bayi dan balita, seperti penimbangan bulanan dan imunisasi. Pada beberapa daerah, Posyandu juga memberikan pelayanan kesehatan untuk masyarakat lansia (lanjut usia).



**Gambar 1.1. Gambaran keseluruhan sistem e-PKK online**

Sistem e-PKK *online* merupakan sistem yang membantu menangani manajemen informasi untuk PKK dan Posyandu, karena di dalam sistem ini terdapat sistem lain yang dikhususkan untuk mengolah dan membantu kinerja kedua komunitas tersebut. Sistem e-PKK *online* terdiri dari sebuah aplikasi “Ensiklopedia Kesehatan Balita dan Ibu Hamil” dan 2 (dua) buah sistem, yaitu sistem PKK dan sistem Posyandu.

Sistem PKK adalah sebuah sistem yang menangani berbagai proses bisnis yang terjadi di dalam sebuah komunitas PKK, seperti mengelola notulensi pertemuan, mengelola iuran PKK, memasukkan data jentik nyamuk, dll. Sistem ini dibagi menjadi dua aplikasi yang dijalankan pada dua *platform* yang berbeda, yaitu satu aplikasi web dan satu aplikasi perangkat bergerak (*mobile*). Aplikasi web PKK dapat diakses oleh pengurus PKK menggunakan akun PKK melalui perangkat komputer atau *laptop*. Aplikasi perangkat bergerak dapat dimiliki oleh seluruh anggota PKK dan dapat diakses melalui perangkat cerdas (*smartphone*).

Sistem Posyandu adalah sebuah sistem yang menangani berbagai proses bisnis yang biasanya terjadi di Posyandu, seperti mengelola data balita, mengelola data ibu balita, mengelola data Posyandu, dan mengelola data keluhan. Sistem ini terdiri dari dua aplikasi dengan *platform* berbeda, yaitu aplikasi web Posyandu dan aplikasi perangkat bergerak (*mobile*) Posyandu. Aplikasi web Posyandu dapat digunakan oleh pengurus Posyandu, sedangkan aplikasi perangkat bergerak Posyandu dapat digunakan oleh ibu balita.

Aplikasi “Ensiklopedia Kesehatan Balita dan Ibu Hamil” merupakan sebuah aplikasi yang menyediakan informasi seputar kesehatan, nutrisi, dan perkembangan untuk balita dan ibu hamil. Aplikasi ini dapat diakses menggunakan perangkat cerdas (*smartphone*) berbasis *Android*.

Sistem e-PKK *online* ini dikembangkan oleh 2 (dua) orang pengembang aplikasi, yaitu penulis dan rekan penulis, Febryan Yeremi Sianipar. Selama masa pengembangan, penulis berfokus pada pengembangan sistem PKK (di dalam garis putus-putus hijau

pada Gambar 1.1) dan rekan penulis berfokus pada pengembangan sistem Posyandu (di dalam garis putus-putus biru pada Gambar 1.1). Aplikasi “Ensiklopedia Kesehatan Balita dan Ibu Hamil” (di dalam garis putus-putus merah muda pada Gambar 1.1) merupakan pengembangan dari aplikasi “Ensiklopedia Kesehatan Balita” milik Kessya Din Dalmi, mahasiswa Jurusan Teknik Informatika Institut Teknologi Sepuluh Nopember angkatan 2010 yang mengembangkan aplikasi ini untuk Tugas Akhir beliau [5]. Pada pengembangan sistem e-PKK *online* ini, aplikasi milik Kessya dikembangkan dengan menambahkan fitur yang menyediakan informasi kesehatan untuk ibu hamil dan dikerjakan oleh kedua pengembang aplikasi, yakni penulis dan rekannya (daerah berwarna merah muda pada Gambar 1.1).

Secara umum, sistem e-PKK *online* ditunjukkan pada Gambar 1.1 dan memiliki ruang lingkup yang sangat besar. Meski begitu, sistem ini masih memiliki kekurangan yang dapat membahayakan pengguna di dalamnya. Pada sistem yang sudah ada, seluruh pengguna dapat mengakses dan mengolah data yang disajikan pada layar perangkat yang digunakan dan pengaturan peran pengguna belum tersedia. Hal ini dapat mengakibatkan ketidakabsahan data yang dimasukkan ke dalam sistem karena pengguna manapun dapat mengolahnya, serta ketidaksesuaian data yang disajikan dengan kebutuhan dan kedudukan pengguna. Selain itu, sistem masih bertukar informasi secara tekstual (murni tanpa pengamanan) yang dapat mengakibatkan kebocoran informasi di antara proses pengiriman dan penerimaan. Diperlukan adanya sebuah pengaturan agar sistem dapat digunakan sesuai dengan peran dan kebutuhan pengguna serta informasi penting dikirimkan secara aman kepada sistem pusat.

Maka dari itu, di sini penulis melakukan pengujian kualitas perangkat lunak sesuai dengan standar ISO 25010. ISO 25010 merupakan salah satu standar penjaminan kualitas perangkat lunak yang di dalamnya mencakup pembahasan mengenai evaluasi dan kebutuhan kualitas sistem dan perangkat lunak (*System and software Quality Requirements and Evaluation – SQuaRE*) [6].

Pengujian dilakukan dengan mengukur metrik kualitas perangkat lunak dan akan menghasilkan nilai yang menunjukkan kualitas perangkat lunak pada karakteristik tertentu. Karakteristik yang diajukan pada Tugas Akhir ini adalah keamanan/sekuritas (*Security*) dengan sub-karakteristik kerahasiaan data (*confidentiality*) dan otentisitas pengguna (*authenticity*). Pemilihan kedua sub-karakteristik ini didasari kekurangan dalam proses komunikasi antar aplikasi di dalam sistem dan proses penyimpanan serta penyaringan informasi oleh sistem, dikarenakan sistem ini menyimpan data-data administrasi komunitas PKK dan Posyandu dan menyimpan informasi kepemilikan data yang disimpan di dalamnya. Selama nilai hasil menunjukkan angka yang dianggap belum memuaskan maka dilakukan perbaikan ke dalam sistem dan diuji kembali hingga mendapatkan nilai yang memuaskan. Penerapan pengujian kualitas diterapkan pada bagian berwarna kuning pada Gambar 1.1, yakni sistem PKK dan sistem Posyandu. Diharapkan pengerjaan Tugas Akhir ini dapat meningkatkan kinerja organisasi yang bersangkutan dengan menyediakan informasi sesuai dengan kebutuhan pengguna dan menjamin kerahasiaan data yang disimpan dan ditukarkan di dalam sistem.

## **1.2. Rumusan Masalah**

Rumusan masalah yang diangkat dalam Tugas Akhir dapat dipaparkan sebagai berikut:

1. Bagaimana hasil pengujian kerahasiaan data dan otentisitas pengguna pada sistem e-PKK *online* yang sudah ada dan apa saja perubahan yang perlu diimplementasikan ke dalam sistem untuk memenuhi kebutuhan pengujian?
2. Bagaimana hasil akhir pengujian kerahasiaan data dan otentisitas pengguna pada sistem e-PKK *online* yang sudah diubah menjadi sistem yang sesuai dengan kedua sub-karakteristik ISO 25010 tersebut?

### 1.3. Batasan Masalah

Permasalahan yang dibahas dalam Tugas Akhir memiliki beberapa batasan antara lain sebagai berikut:

1. Standar yang digunakan adalah ISO 25010.
2. Sub-karakteristik yang diukur, diimplementasikan, dan diujikan kembali pada sistem adalah sub-karakteristik kerahasiaan data (*confidentiality*) dan otentisitas pengguna (*authenticity*) yang merupakan bagian dari karakteristik sekuritas ISO 25010.
3. Sistem yang digunakan adalah sistem PKK dan sistem Posyandu, yang merupakan bagian dari sistem e-PKK *online* serta terdiri dari aplikasi web dan aplikasi perangkat bergerak (*mobile*).
4. Aplikasi web dikembangkan menggunakan kerangka kerja *Laravel* versi 5.1.
5. Aplikasi perangkat bergerak dikembangkan menggunakan kerangka kerja *PhoneGap*.
6. Sistem merupakan penerapan sistem *Client-Server*.
7. Basis data yang digunakan sistem ini menggunakan *MySQL*.

### 1.4. Tujuan

Tujuan dari pembuatan Tugas Akhir ini adalah sebagai berikut:

1. Didapatkan hasil pengujian kerahasiaan data dan otentisitas pengguna dan perancangan proses apa saja yang perlu diimplementasikan ke dalam sistem untuk memenuhi kedua sub-karakteristik ISO 25010 tersebut.
2. Didapatkan pengukuran sekuritas data dan otentisitas pengguna sesuai dengan metrik yang ada dan dinilai sistem e-PKK *online* yang dimodifikasi sudah memenuhi standar ISO 25010 sesuai dengan sub-karakteristik yang diujikan.

### 1.5. Metodologi

Tahap yang dilakukan untuk menyelesaikan Tugas Akhir ini adalah sebagai berikut:

#### 1. Penyusunan proposal Tugas Akhir

Tahap awal dalam proses pengerjaan Tugas Akhir ini adalah penyusunan proposal Tugas Akhir. Pada proposal Tugas Akhir ini diajukan pengembangan, pengukuran, perbaikan, dan pengujian sub-karakteristik kerahasiaan data (*confidentiality*) dan sub-karakteristik otentisitas pengguna (*authenticity*) dari karakteristik sekuritas pada model kualitas perangkat lunak ISO 25010 menggunakan studi kasus sistem e-PKK *online*.

#### 2. Studi literatur

Pengerjaan Tugas Akhir ini membutuhkan pemahaman terhadap beberapa literatur yang mendukung, seperti pemahaman ISO 25010, cara menguji dan menyimpulkan hasil pengujian dari penerapan, dan memahami informasi-informasi apa saja yang perlu untuk diberi perlakuan kerahasiaan data.

#### 3. Analisis dan Desain Perangkat Lunak

Sistem e-PKK *online* terdiri dari dua buah sistem, yakni sistem PKK dan sistem Posyandu. Kedua sistem tersebut terbagi menjadi dua buah aplikasi dengan *platform* yang berbeda, yakni aplikasi web dan aplikasi perangkat bergerak yang dapat diakses menggunakan perangkat cerdas.

Aplikasi web PKK menyediakan beberapa fitur sebagai berikut:

- Mengelola data PKK
- Mengelola data periode PKK
- Mengelola data jabatan PKK

- Mengelola data pengurus PKK
- Mengelola data anggota PKK
- Mengelola kas PKK
- Mengelola absen PKK
- Mengelola notulensi
- Mengelola pengumuman
- Mengelola data laporan bidang
- Mengelola data jentik nyamuk
- Mengelola keluhan dan komentar
- Mengelola pengguna sistem

Aplikasi perangkat bergerak PKK menyediakan beberapa fitur sebagai berikut:

- Melihat laporan iuran
- Mengolah data jentik nyamuk
- Melihat notulensi pertemuan rutin
- Melihat pengumuman
- Mengolah keluhan dan komentar
- Mengelola akun pengguna

Aplikasi web Posyandu menyediakan beberapa fitur sebagai berikut:

- Mengelola data balita
- Mengelola data ibu balita
- Mengelola data penimbangan balita
- Mengelola data pemberian imunisasi
- Mengelola data pemberian kapsul
- Mengelola data pengurus Posyandu
- Mengelola data kas Posyandu
- Mengelola data absen balita
- Mengelola data keluhan
- Mengelola data jawaban keluhan



Aplikasi perangkat bergerak Posyandu menyediakan beberapa fitur sebagai berikut:

- Melihat rekomendasi nutrisi balita
- Melihat informasi perkembangan balita
- Melihat informasi pertolongan pertama pada kecelakaan balita
- Memasukkan dan melihat data balita
- Memasukkan dan melihat keluhan

#### **4. Implementasi Perangkat Lunak**

Implementasi sistem e-PKK *online* pada sub-karakteristik kerahasiaan data dan otentisitas pengguna merupakan tahapan utama untuk membangun bagian kecil dari sistem yang dapat menangani manajemen hak akses pengguna. Penerapan kerahasiaan data akan dilakukan pada fitur manajemen pengelolaan akun pengguna, pengaturan hak akses untuk fitur yang disediakan, dan pengamanan informasi penting antar aplikasi dalam satu sistem. Penerapan otentikasi pengguna akan dilakukan pada fitur *login* dan verifikasi akun pengguna perangkat bergerak. Dalam pengerjaan Tugas Akhir ini menggunakan *editor* teks *Sublime Text 3*, aplikasi *web server XAMPP*, kerangka kerja *website Laravel* versi 5.1, dan bahasa pemrograman PHP.

#### **5. Pengujian dan Evaluasi**

Tahap pengujian dan evaluasi akan dilakukan dalam beberapa cara di antaranya adalah sebagai berikut:

##### **1. Pengujian Fungsionalitas**

Pengujian fungsionalitas menggunakan metoda kotak hitam (*blackbox testing*), di mana metode ini dilakukan untuk memastikan kesesuaian hasil keluaran

sistem. Pengujian fungsionalitas dilakukan dengan menyiapkan sejumlah skenario sebagai tolak ukur keberhasilan pengujian. Fungsionalitas yang diujikan pada pengujian ini adalah fungsionalitas-fungsionalitas yang berkaitan dengan pengujian kerahasiaan data dan otentisitas pengguna pada tahap perancangan.

2. Pengujian Kerahasiaan Data dan Otentisitas Pengguna menggunakan ISO 25010

Pengujian kerahasiaan data dan otentisitas pengguna berdasarkan ISO 25010 menggunakan metrik yang telah disediakan di dalamnya untuk menilai kualitas pengamanan kerahasiaan data suatu perangkat lunak. Metrik yang diujikan adalah kemampuan pengendalian akses, ketepatan enkripsi data, kekuatan kriptografi algoritma, kesesuaian protokol otentikasi, dan kesesuaian aturan otentikasi.

## **6. Penyusunan Buku Tugas Akhir**

Pada tahap ini dilakukan penyusunan laporan yang menjelaskan dasar teori dan metode yang digunakan dalam Tugas Akhir ini serta hasil dari implementasi aplikasi perangkat lunak yang telah dibuat. Sistematika penulisan buku Tugas Akhir secara garis besar antara lain:

1. Pendahuluan
  - a. Latar Belakang
  - b. Rumusan Masalah
  - c. Batasan Tugas Akhir
  - d. Tujuan
  - e. Metodologi
  - f. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Pengujian dan Evaluasi

5. Kesimpulan dan Saran
6. Daftar Pustaka

### **1.6. Sistematika Penulisan**

Buku Tugas Akhir ini terdiri atas beberapa bab yang tersusun secara sistematis, yaitu sebagai berikut.

1. Bab I. Pendahuluan  
Bab pendahuluan berisi penjelasan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan, manfaat dan sistematika penulisan Tugas Akhir.
2. Bab II. Tinjauan Pustaka  
Bab tinjauan pustaka berisi penjelasan mengenai dasar teori yang mendukung pengerjaan Tugas Akhir.
3. Bab III. Analisis dan Perancangan  
Bab analisis dan perancangan berisi penjelasan mengenai alur pengujian standar kualitas dan rancangan implementasi kerahasiaan data dan otentisitas pengguna pada sistem yang telah ada.
4. Bab IV. Implementasi  
Bab implementasi berisikan proses-proses yang diimplementasikan ke dalam sistem. Proses-proses yang dituliskan di dalam bab ini sesuai dengan perancangna yang direncanakan pada bab sebelumnya.
5. Bab V. Uji Coba dan Evaluasi  
Bab uji coba dan evaluasi berisi pembahasan mengenai uji coba fungsionalitas yang diimplementasikan ke dalam sistem sesuai dengan perancangan dan hasil dari uji coba ISO 25010 yang dilakukan pada sistem e-PKK *online*.
6. Bab VI. Kesimpulan dan Saran  
Bab kesimpulan dan saran berisi kesimpulan hasil penelitian. Selain itu, bagian ini berisi saran untuk pengerjaan lebih lanjut atau permasalahan yang dialami dalam proses pengerjaan Tugas Akhir.

*[Halaman ini sengaja dikosongkan]*

## **BAB II**

### **TINJAUAN PUSTAKA**

Bab ini membahas penjelasan teori yang menjadi dasar dalam pembuatan Tugas Akhir ini. Teori yang mendukung pengerjaan Tugas Akhir ini dijelaskan pada subbab-subbab berikut.

#### **2.1. Sistem e-PKK Online**

Sistem e-PKK *online* merupakan sebuah sistem dengan skala nasional yang terdiri dari 2 (dua) buah sub-sistem, yakni sistem PKK dan sistem Posyandu, serta sebuah aplikasi “Ensiklopedia Kesehatan Balita dan Ibu Hamil.” Layanan sistem e-PKK *online* dikembangkan karena kebutuhan dalam hal manajemen informasi mengenai data layanan dan administrasi masyarakat. Layanan sistem e-PKK *online* ini menggunakan sebuah *server* yang diletakkan pada *server* Workshop Pemrograman 2 Jurusan Teknik Informatika Institut Teknologi Sepuluh Nopember dan dapat diakses pada tautan berikut: <http://epkk.if.its.ac.id>.

Sistem PKK adalah sebuah sistem yang menangani berbagai proses bisnis yang terjadi di dalam sebuah organisasi PKK, seperti mengelola notulensi pertemuan, mengelola iuran PKK, memasukkan data jentik nyamuk, dll. Sistem ini terdiri dari 2 (dua) aplikasi dengan *platform* yang berbeda, yaitu aplikasi web dan aplikasi perangkat bergerak. Aplikasi web PKK dapat diakses oleh pengurus PKK melalui aplikasi *browser* komputer, *laptop*, atau HP. Aplikasi perangkat bergerak dapat dimiliki oleh seluruh anggota PKK dan dapat diakses melalui perangkat cerdas (*smartphone*) masing-masing individu.

Sistem Posyandu adalah sebuah sistem yang menangani berbagai proses bisnis yang biasanya terjadi di Posyandu, seperti mengelola data balita, mengelola data ibu balita, mengelola data Posyandu, dan mengelola data keluhan. Sistem ini terdiri dari 2 (dua) aplikasi dengan *platform* berbeda, yaitu aplikasi web Posyandu dan aplikasi perangkat bergerak Posyandu. Aplikasi web

Posyandu dapat digunakan oleh pengurus Posyandu, sedangkan aplikasi perangkat bergerak Posyandu dapat digunakan oleh ibu balita.

## **2.2. ISO 25010**

ISO (*International Organization for Standardization*) 25010 merupakan bagian dari sebuah serangkaian standar ISO 25000, yang lebih dikenal dengan singkatan *SQuaRE* (*System and Software Quality Requirements and Evaluation* / Evaluasi dan Kebutuhan kualitas Sistem dan Perangkat Lunak) [7]. Serangkaian standar ini memiliki tujuan untuk menciptakan sebuah kerangka kerja untuk melakukan evaluasi terhadap kualitas produk perangkat lunak. ISO 25000 merupakan hasil dari perkembangan beberapa standar lainnya; terutama berawal dari ISO 9126, yang menjelaskan sebuah model kualitas untuk evaluasi produk perangkat lunak, dan ISO 14598, yang menjelaskan tentang proses evaluasi produk perangkat lunak. Serangkaian standar ISO 25000 terdiri dari lima buah divisi, yang di mana ISO 25010 merupakan salah satu di antaranya.

ISO 25010 merupakan sebuah divisi yang ada untuk menjelaskan model-model kualitas untuk sistem komputer dan produk perangkat lunak, kualitas penggunaan, dan data. ISO 25010 – Model Kualitas Sistem dan Perangkat Lunak – menjelaskan model, terdiri dari karakteristik dan sub-karakteristik, untuk kualitas produk perangkat lunak dan kualitas penggunaan perangkat lunak.

Model kualitas adalah landasan dari sebuah sistem evaluasi kualitas produk. Model kualitas menjelaskan karakteristik kualitas yang tepat untuk diterapkan pada saat melakukan evaluasi akan atribut sebuah produk perangkat lunak. Kualitas sebuah sistem adalah satuan yang harus disediakan untuk memenuhi kebutuhan sistem yang berasal dari beragam pemegang kepentingan dan memiliki nilai. Beberapa kebutuhan pemegang kepentingan (fungsionalitas, performa, sekuritas, dll.) sudah direpresentasikan di dalam model kualitas, yang menggolongkan kualitas produk menjadi karakteristik dan sub-karakteristik. Model kualitas produk

yang dijelaskan pada ISO 25010 meliputi delapan karakteristik kualitas yang ditunjukkan pada Gambar 2.1.



**Gambar 2.1. Model Kualitas Perangkat Lunak ISO 25010**

Pada pengerjaan Tugas Akhir ini, penulis menerapkan dua sub-karakteristik pada model kualitas perangkat lunak ISO 25010 pada karakteristik Sekuritas, yakni kerahasiaan data (*confidentiality*) dan otentisitas pengguna (*authenticity*).

### 2.3. Kerahasiaan Data (*Confidentiality*)

Kerahasiaan data merupakan sebuah satuan di mana sebuah produk atau sistem memastikan bahwa informasi/data hanya dapat diakses oleh pengguna yang memiliki otoritas untuk mengakses. Satuan yang harus disediakan produk perangkat lunak adalah perlindungan akan penyebaran data atau informasi oleh pengguna yang tidak terotorisasi, baik secara tidak sengaja maupun disengaja [6].

Pengukuran kerahasiaan data digunakan untuk menilai tingkat sebuah produk atau sistem dalam memastikan bahwa data hanya dapat diakses oleh pengguna yang memiliki otorisasi untuk mengakses data tersebut. Pengukuran kerahasiaan data dapat dilakukan dengan menilai tiga satuan, yakni kemampuan pengendalian akses, ketepatan enkripsi data, dan kekuatan kriptografi algoritma.

**Kemampuan pengendalian akses.** Satuan ini mengukur proporsi dari kerahasiaan data yang dilindungi dari akses yang tidak terotorisasi. Perhitungan satuan ini dilakukan dengan:

$$X_{KPA} = 1 - \left( \frac{A_{KPA}}{B_{KPA}} \right)$$

Keterangan:

- $X_{KPA}$  = Nilai metrik kemampuan pengendalian akses dalam rentang 1 (tinggi) hingga 0 (rendah)
- $A_{KPA}$  = Jumlah data yang dapat diakses tanpa otorisasi khusus
- $B_{KPA}$  = Jumlah data yang membutuhkan pengendalian akses

**Ketepatan enkripsi data.** Satuan ini mengukur seberapa tepatnya enkripsi/dekripsi dari data yang diimplementasikan secara tertulis pada spesifikasi kebutuhan perangkat lunak. Perhitungan satuan ini dilakukan dengan:

$$X_{KED} = \frac{A_{KED}}{B_{KED}}$$

Keterangan:

- $X_{KED}$  = Nilai metrik ketepatan enkripsi data dalam rentang 1 (tinggi) hingga 0 (rendah)
- $A_{KED}$  = Jumlah data yang tepat dienkrpsi/didekripsi
- $B_{KED}$  = Jumlah data yang butuh dienkrpsi/didekripsi

**Kekuatan kriptografi algoritma.** Satuan ini mengukur seberapa banyak algoritma kriptografi yang melakukan pemeriksaan dengan baik dan digunakan di dalam sistem. Kriptografi adalah ilmu mengenai teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa data pribadi dan otentikasi. Contoh implementasi/algoritma kriptografi yang umum digunakan antara lain: DES, RSA, *Hashing*, MD5, AES, SHA-1, dan HMAC. Perhitungan satuan ini dilakukan dengan:

$$X_{KKA} = 1 - \left( \frac{A_{KKA}}{B_{KKA}} \right)$$

Keterangan:

- $X_{KKA}$  = Nilai metrik kekuatan kriptografi algoritma dalam rentang 1 (tinggi) hingga 0 (rendah)



- $A_{KKA}$  = Jumlah algoritma kriptografi yang rusak atau berisiko apabila digunakan
- $B_{KEKA}$  = Jumlah algoritma kriptografi yang digunakan

## 2.4. Otentisitas Pengguna (*Authenticity*)

Otentisitas merupakan sebuah satuan yang mengidentifikasi sebuah subjek atau sumber daya yang dapat dibuktikan sebagai pemiliknya [6]. Otentikasi merupakan proses untuk mengenali identitas sebuah subjek atau sumber daya sesuai dengan fakta yang diberikan [8]. Pengukuran otentisitas dapat dilakukan dengan menilai dua satuan, yakni kesesuaian protokol otentikasi dan kesesuaian aturan otentikasi.

**Kesesuaian protokol otentikasi.** Satuan ini menilai seberapa baik sistem mengenali identitas subjek atau sumber daya. Perhitungan satuan ini dilakukan dengan:

$$X_{KPO} = \frac{A_{KPO}}{B_{KPO}}$$

Keterangan:

- $X_{KPO}$  = Nilai metrik kesesuaian protokol otentikasi dalam rentang 1 (tinggi) hingga 0 (rendah)
- $A_{KPO}$  = Jumlah protokol otentikasi yang disediakan (ID pengguna, kata sandi, dll.)
- $B_{KPO}$  = Jumlah protokol otentikasi yang dibutuhkan pada tahap spesifikasi

**Kesesuaian aturan otentikasi.** Satuan ini mengukur proporsi kebutuhan aturan otentikasi yang digunakan untuk sistem yang aman. Otentikasi adalah verifikasi yang menentukan apakah seseorang memiliki hak. Biasanya melibatkan nama pengguna (*username*) dan kata sandi (*password*), atau menggunakan metode lain yang menunjukkan identitas seperti sidik jari, dll [9]. Perhitungan satuan ini dilakukan dengan:

$$X_{KAO} = \frac{A_{KAO}}{B_{KAO}}$$

Keterangan:

- $X_{KAO}$  = Nilai metrik kesesuaian aturan otentikasi dalam rentang 1 (tinggi) hingga 0 (rendah)
- $A_{KAO}$  = Jumlah aturan otentikasi yang diimplementasikan
- $B_{KAO}$  = Jumlah aturan otentikasi yang dibutuhkan sebuah sistem yang aman

## 2.5. Kerangka Kerja *Laravel*

Kerangka kerja *Laravel* merupakan kerangka kerja yang dikembangkan menggunakan bahasa pemrograman PHP dan diciptakan oleh Taylor Otwell di bawah lisensi MIT [10]. Kerangka kerja ini dikhususkan untuk pengembang aplikasi web. Fitur yang disediakan oleh kerangka kerja ini mempermudah kinerja pengembang aplikasi dan juga kinerja web itu sendiri, terutama pada bagian akses basis data.

*Laravel* menggunakan pola arsitektur MVC (*Model – View – Controller*), yakni pola yang membagi aplikasi perangkat lunak menjadi tiga bagian yang berhubungan dan memiliki fungsi masing-masing. *Model* menangani komunikasi dengan media penyimpanan data. *View* menangani komunikasi yang diberikan oleh pengguna ke dalam aplikasi dan sebaliknya. *Controller* menangani proses bisnis pertukaran informasi antara *model* dan *view* serta pengolahan data agar menjadi informasi yang dapat diterima oleh pengguna maupun penyimpanan data.

## 2.6. Kerangka Kerja *PhoneGap*

PhoneGap adalah sebuah kerangka kerja pembuatan aplikasi perangkat bergerak berbasis sumber terbuka yang dikeluarkan oleh sebuah perusahaan di Amerika yang bernama Nitobi. Kerangka kerja *PhoneGap* memungkinkan seseorang mengembangkan aplikasi perangkat bergerak dengan menggunakan keahlian HTML, CSS, dan *JavaScript* [11]. Sebuah aplikasi yang dibuat dengan menggunakan kerangka kerja *PhoneGap* dapat dikembangkan ke berbagai *platform*. *Platform* yang didukung oleh *PhoneGap* antara lain iOS, Android, Windows Mobile, Blackberry, WebOS, Symbian, dan Bada.

## **BAB III**

### **ANALISIS DAN PERANCANGAN**

Bab ini menjelaskan analisis dan perancangan perangkat lunak untuk mencapai tujuan dari pengerjaan Tugas Akhir ini. Analisis yang dilakukan adalah analisis terhadap sistem e-PKK *online* yang sudah ada. Perancangan yang dijelaskan meliputi perancangan proses pengujian ISO, perancangan manajemen kerahasiaan data dan otentisitas pengguna, perancangan fitur yang berkaitan dengan metrik yang diujikan, dan perancangan antarmuka pengguna.

#### **3.1. Analisis Sistem e-PKK Online**

Sistem e-PKK *online* terdiri dari 2 (dua) buah sistem, yaitu sistem PKK dan sistem Posyandu, dan sebuah aplikasi “Ensiklopedia Kesehatan Balita dan Ibu Hamil” sebagai pendukung dan penyedia informasi seputar kesehatan balita dan ibu hamil. Kedua sistem terdiri dari sebuah aplikasi web dan sebuah aplikasi perangkat bergerak. Kebutuhan fungsionalitas, kasus penggunaan, dan deskripsi kasus penggunaan aplikasi web PKK dapat dilihat pada **LAMPIRAN A.1. Kebutuhan Sistem PKK Online**. Penjelasan mengenai aplikasi perangkat bergerak PKK selengkapnya dapat dibaca pada Buku Kerja Praktik milik penulis [12] dan penjelasan mengenai sistem Posyandu selengkapnya dapat dibaca pada Buku pengerjaan Tugas Akhir milik rekan penulis, Febryan Yeremi Sianipar [13].

Aplikasi Ensiklopedia Kesehatan Balita dan Ibu Hamil merupakan aplikasi yang berisikan informasi statis mengenai kesehatan untuk balita dan ibu hamil. Sebelumnya aplikasi ini dikembangkan oleh Kessya Din Dalmi untuk fitur-fitur yang berhubungan dengan kesehatan balita dan pada perkembangan sistem e-PKK *online* ditambahkan fitur-fitur mengenai kesehatan ibu hamil. Fitur-fitur mengenai kesehatan balita dijelaskan lebih lengkap pada Buku pengerjaan Tugas Akhir milik Kessya Din Dalmi [5]. Penambahan fitur-fitur mengenai kesehatan ibu hamil

yang dikerjakan oleh penulis dapat dilihat pada Tabel 7.17. Terdapat fitur tambahan lain yang dikerjakan oleh rekan penulis, Febryan Yeremi Sianipar, dan dapat dilihat pada Buku pengerjaan Tugas Akhir milik rekan penulis [13], antara lain mendapatkan daftar makanan untuk ibu hamil dan melihat rekomendasi makanan untuk ibu hamil.

Sistem e-PKK *online* juga memiliki kebutuhan lainnya, antara lain kebutuhan non-fungsional dan basis data sistem. Kebutuhan non-fungsional sistem e-PKK *online* dapat dilihat pada Tabel 7.18. Model fisik basis data sistem e-PKK *online* dapat dilihat pada **LAMPIRAN A.2. Basis Data Sistem e-PKK Online.**

Pada subbab-subbab berikut akan dijelaskan kerahasiaan data dan otentisitas pengguna pada sistem yang telah ada. Penjabaran ini bertujuan untuk mengetahui kekurangan aplikasi yang ada sehingga didapatkan perancangan untuk mengelola kedua sub-karakteristik ISO 25010 tersebut.

### **3.1.1. Kerahasiaan Data Sistem**

Sistem e-PKK *online* yang sudah ada bersifat sangat terbuka untuk pengguna, di mana seluruh pengguna dapat mengakses data apapun dan milik siapapun. Hal ini dapat menyebabkan terjadinya perubahan data milik komunitas daerah lain, baik secara sadar maupun tidak. Sifat terbuka ini juga memperlihatkan informasi yang dimiliki komunitas daerah lain, seperti informasi kas yang merupakan informasi pribadi yang hanya berhak diketahui oleh pemilik informasi.

Proses kriptografi pada sistem yang sudah ada berjalan dengan lancar dan menghasilkan keluaran yang tepat. Algoritma kriptografi yang digunakan pada sistem adalah fungsi *Hash* milik kerangka kerja pihak ketiga, *Sentinel 2.0*. Kriptografi tersebut menjaga kerahasiaan kata sandi akun pribadi pada basis data sistem. Hanya saja, fungsi *Hash* tersebut tidak bisa digunakan pada aplikasi perangkat bergerak. Aplikasi perangkat bergerak pada tiap sistem masih bertukar informasi penting, seperti kata sandi, dalam bentuk tekstual tanpa adanya pengamanan informasi (enkripsi). Hal ini dapat menyebabkan, kebocoran informasi kata sandi dan

penyalahgunaan akun dan kata sandi untuk merubah data di dalam sistem. Ketidakmampuan mengakses fungsi *Hash* dikarenakan perbedaan bahasa pemrograman yang digunakan aplikasi web dan aplikasi perangkat bergerak. Perlu adanya sebuah proses tertentu agar komunikasi antar *platform* dapat berjalan aman dan data penting pengguna tidak dengan mudah dapat diakses pihak selain pengguna yang memiliki.

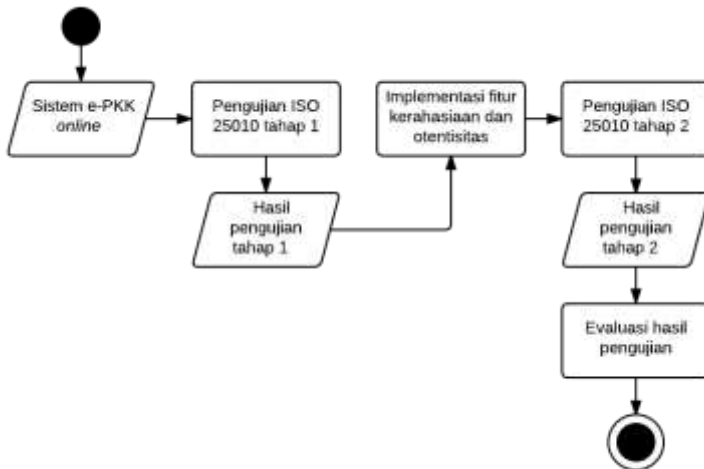
### 3.1.2. Otentikasi Pengguna Sistem

Kedua sub-sistem e-PKK *online* dihubungkan dengan sebuah sistem kerangka kerja pihak ketiga yang bernama *Sentinel 2.0*. *Sentinel 2.0* merupakan sebuah kerangka kerja yang bergantung pada kerangka kerja *Laravel* dan berfungsi menangani otorisasi dan otentikasi serta fitur-fitur yang mendukung proses tersebut [14]. Pada implementasinya, *Sentinel 2.0* sering melontarkan pesan kekeliruan (*error*) karena gangguan koneksi, meskipun koneksi pada pihak pengguna tidak mengalami masalah begitu pula pada pihak penyedia (*server*). Selain itu, *Sentinel 2.0* memiliki konfigurasi yang rumit dan kelas yang saling bergantung satu sama lain, serta tidak memiliki dokumentasi yang lengkap, sehingga apabila pengembang melakukan sedikit perubahan terhadap kerangka kerja tersebut maka dapat terjadi kemungkinan adanya kesalahan di proses otentikasi karena konfigurasi yang tidak tepat.

Pada sistem e-PKK *online* yang sudah ada, sudah disediakan sarana untuk mengenali pengguna, yaitu fitur *login*. Fitur *login* yang disediakan belum bisa mengenali pengguna karena tidak adanya pembeda antar pengguna, seperti peran atau ID pengguna, sehingga seluruh pengguna yang *login* ke dalam salah satu sistem dianggap sama. Selain itu, aturan otentikasi yang disediakan masih sedikit. Aturan otentikasi yang diperlukan untuk memenuhi kebutuhan sistem e-PKK *online* antara lain fitur *login*, registrasi pengguna, mengubah kata sandi, mengenali peran pengguna, dan mengenali pengguna baru. Di antara beberapa kebutuhan tersebut, hanya fitur *login* pada aplikasi web dan mengubah kata sandi pada aplikasi perangkat bergerak PKK yang telah diimplementasikan.

### 3.2. Perancangan Pengujian ISO 25010

Pengujian sistem e-PKK *online* akan dilakukan melalui perhitungan nilai metrik kualitas perangkat lunak sesuai dengan standar ISO 25010. Metrik yang diujikan adalah metrik sub-karakteristik kerahasiaan data dan otentisitas pengguna, seperti yang dicantumkan pada Bab 2.3 dan Bab 2.4. Tiap metrik memiliki karakteristik yang sama, yakni memiliki nilai kepuasan tertinggi bernilai 1 (satu) dan nilai kepuasan terendah bernilai 0 (nol). Oleh karena itu, untuk memiliki sistem bermutu bagus diperlukan pengujian dengan keseluruhan hasil perhitungan metrik berupa nilai dengan kepuasan tertinggi.



**Gambar 3.1. Diagram Alir Pengujian ISO 25010**

Pengujian ISO 25010 dengan metrik yang ditentukan akan dilakukan dalam 2 (dua) tahap. Tahap pertama adalah perhitungan metrik ISO 25010 terhadap sistem e-PKK *online* yang sudah ada. Tahap ini dilakukan untuk mendapatkan nilai perhitungan awal yang akan dibandingkan dengan nilai perhitungan pada sistem yang sudah dimodifikasi. Tahap kedua adalah perhitungan metrik ISO 25010 terhadap sistem yang sudah dimodifikasi. Tahap ini

dapat menentukan apakah modifikasi yang diimplementasikan ke dalam sistem memberikan dampak terhadap perubahan nilai perhitungan metrik ISO 25010 yang sudah ditentukan. Alur pengujian dapat dilihat pada Gambar 3.1.

Perhitungan metrik kemampuan pengendalian akses akan dilakukan dengan menghitung jumlah jalur (*route*) yang disediakan sistem agar pengguna dapat mengakses sebuah halaman dan dinilai perlu untuk diberi otorisasi khusus untuk mengakses halaman tersebut. Lalu, tiap jalur akan dilihat apakah sudah diberi otorisasi khusus untuk mengakses jalur tersebut. Jalur yang sudah diberi otorisasi khusus tidak akan dihitung karena metrik ini memerlukan jumlah jalur yang dapat diakses tanpa otorisasi khusus. Pengujian apakah suatu jalur sudah diberi otorisasi khusus dapat dilakukan dengan mengakses halaman tersebut dengan/tanpa otorisasi yang tepat. Selanjutnya, jumlah keseluruhan jalur yang perlu diberi otorisasi khusus dan jumlah jalur yang belum diberi otorisasi khusus akan dimasukkan ke dalam variabel metrik kemampuan pengendalian akses dan didapatkan nilai metrik ini. Contoh perhitungan metrik ini dapat dilihat pada Tabel 3.1.

**Tabel 3.1. Contoh Perhitungan Metrik Kemampuan Pengendalian Akses**

Jalur	Perlu otorisasi?	Status	Implementasi otorisasi
A	Tidak	Tidak dihitung	-
B	Perlu	Dihitung	Belum
C	Perlu	Dihitung	Sudah
Jumlah jalur yang perlu otorisasi ( $B_{KPA}$ )			2
Jumlah jalur yang belum diberi otorisasi ( $A_{KPA}$ )			1
Hasil perhitungan			$1 - \frac{1}{2} = 0,5$

Perhitungan metrik ketepatan enkripsi data akan dilakukan dengan menghitung jumlah data yang dienkripsi/didekripsi. Lalu, tiap data yang didapatkan akan dilihat apakah sudah dienkripsi/didekripsi dengan benar. Pengujian apakah suatu data sudah dienkripsi dengan benar adalah dengan melakukan proses

dekripsi pada data tersebut, begitu pula sebaliknya. Pengujian tidak perlu menampilkan hasil enkripsi ataupun dekripsi, tetapi dapat dilakukan dengan memanfaatkan fitur-fitur yang tersedia di dalam sistem, seperti registrasi untuk pengujian enkripsi data dan *login* untuk dekripsi data. Selanjutnya, jumlah data yang perlu dienkripsi/didekripsi dan jumlah data yang sudah tepat dienkripsi/didekripsi akan dimasukkan ke dalam variabel metrik ketepatan enkripsi data dan didapatkan nilai metrik ini. Contoh perhitungan metrik ini dapat dilihat pada Tabel 3.2.

**Tabel 3.2. Contoh Perhitungan Metrik Ketepatan Enkripsi Data**

Data	Perlu dienkripsi / didekripsi?	Status	Tepat dienkripsi / didekripsi
A	Tidak	Tidak dihitung	-
B	Perlu	Dihitung	Tidak
C	Perlu	Dihitung	Tepat
Jumlah data yang perlu dienkripsi/didekripsi ( $B_{KED}$ )			2
Jumlah data yang tepat dienkripsi/didekripsi ( $A_{KED}$ )			1
Hasil perhitungan			$\frac{1}{2} = 0,5$

Perhitungan metrik kekuatan kriptografi algoritma akan dilakukan dengan menghitung jumlah fungsi kriptografi yang digunakan di dalam sistem dan menghasilkan keluaran yang tepat. Pengujian ketepatan kriptografi dapat dibuktikan dengan melakukan proses yang sama dengan pengujian pada metrik ketepatan enkripsi data. Apabila penggunaan fungsi sudah menghasilkan keluaran yang tepat maka fungsi tersebut dianggap tidak rusak atau tidak berisiko apabila digunakan. Selanjutnya, jumlah fungsi tersebut akan dimasukkan ke dalam variabel metrik kekuatan kriptografi algoritma dan didapatkan nilai metrik ini. Contoh perhitungan metrik ini dapat dilihat pada Tabel 3.3.

**Tabel 3.3. Contoh Perhitungan Metrik Kekuatan Kriptografi Algoritma**

Fungsi	Digunakan di dalam sistem?	Status	Keluaran tepat?
A	Tidak	Tidak dihitung	-
B	Ya	Dihitung	Tidak



Fungsi	Digunakan di dalam sistem?	Status	Keluaran tepat?
C	Ya	Dihitung	Tepat
Jumlah fungsi kriptografi yang digunakan ( $B_{KKA}$ )			2
Jumlah fungsi dengan keluaran tepat ( $A_{KKA}$ )			1
Hasil perhitungan			$1 - \frac{1}{2} = 0,5$

Perhitungan metrik kesesuaian protokol otentikasi akan dilakukan dengan menghitung jumlah data yang dianggap sebagai protokol otentikasi. Lalu, tiap data tersebut akan diperiksa apakah sudah digunakan di dalam sistem sebagai salah satu protokol otentikasi. Pengujian dapat dilakukan dengan melakukan otentikasi pengguna menggunakan data protokol otentikasi tersebut. Selanjutnya, jumlah protokol otentikasi yang digunakan dan dibutuhkan akan dimasukkan ke dalam variabel metrik kesesuaian protokol otentikasi dan didapatkan nilai metrik ini. Contoh perhitungan metrik ini dapat dilihat pada Tabel 3.4.

**Tabel 3.4. Contoh Perhitungan Metrik Kesesuaian Protokol Otentikasi**

Protokol otentikasi	Dibutuhkan sebagai protokol?	Digunakan di dalam sistem?
A	Tidak	-
B	Dibutuhkan	Tidak
C	Dibutuhkan	Digunakan
Jumlah protokol yang dibutuhkan ( $B_{KPO}$ )		2
Jumlah protokol yang digunakan ( $A_{KPO}$ )		1
Hasil perhitungan		$\frac{1}{2} = 0,5$

Perhitungan metrik kesesuaian aturan otentikasi akan dilakukan dengan menghitung jumlah fitur yang disediakan sistem yang berhubungan dengan proses otentikasi. Aturan otentikasi perlu untuk dispesifikasikan terlebih dahulu sesuai dengan kebutuhan sistem. Dalam kasus sistem e-PKK *online*, aturan otentikasi yang diperlukan adalah *login*, registrasi pengguna baru, mengubah kata sandi, perangkat tengah untuk aplikasi web, dan

verifikasi akun pengguna untuk aplikasi perangkat bergerak. Lalu, tiap aturan otentikasi diperiksa apakah sudah diimplementasikan ke dalam sistem. Selanjutnya, jumlah aturan otentikasi yang diimplementasikan dan dibutuhkan sistem akan dimasukkan ke dalam variabel metrik kesesuaian aturan otentikasi dan didapatkan nilai metrik ini. Contoh perhitungan metrik ini dapat dilihat pada.

**Tabel 3.5. Contoh Perhitungan Metrik Kesesuaian Aturan Otentikasi**

<i>Platform</i>	<i>Aturan Otentikasi</i>	<b>Sistem PKK</b>	<b>Sistem Posyandu</b>	<b>Total</b>
Web	Login	V	V	2
	Registrasi	X	X	0
	Ubah Kata Sandi	X	X	0
	Perangkat Tengah	V	X	1
Perangkat Bergerak	Login	V	V	2
	Registrasi	X	X	0
	Ubah Kata Sandi	V	X	1
	Verifikasi Akun	X	X	0
Jumlah aturan yang dibutuhkan ( $B_{KAO}$ )			16	
Jumlah aturan yang diimplementasikan ( $A_{KPO}$ )			6	
Hasil perhitungan			$\frac{6}{16} = 0,375$	

### 3.3. Perancangan Manajemen Kerahasiaan Data

Metrik kerahasiaan data (*confidentiality*) pada ISO 25010 melingkupi informasi yang sesuai dan dibutuhkan pengguna, enkripsi informasi yang dipertukarkan tiap aplikasi, dan algoritma kriptografi yang digunakan. Berikut adalah beberapa kemungkinan pada fitur-fitur sistem yang memungkinkan terjadinya kebocoran kerahasiaan beserta perencanaan proses untuk mengatasinya:

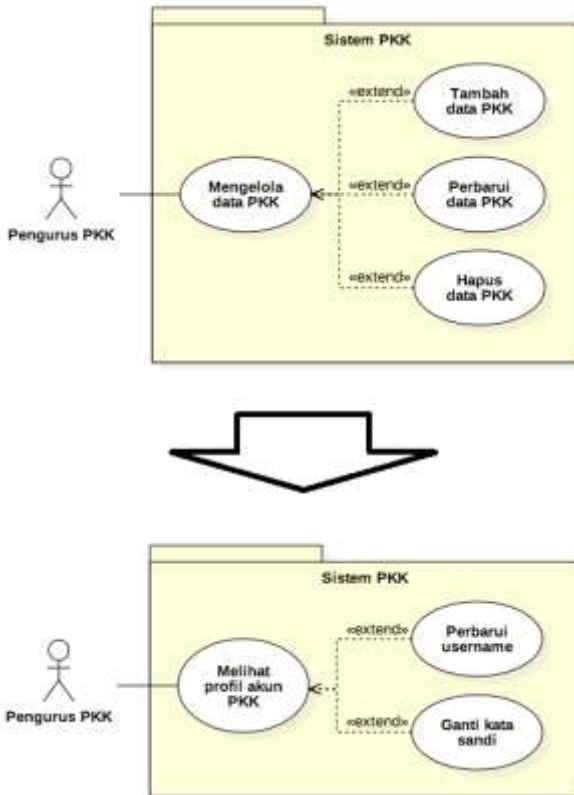
- Membuka suatu halaman web/fitur aplikasi

Kebocoran kerahasiaan data sangat memungkinkan terjadi pada saat memuat halaman web/fitur aplikasi tertentu. Perlu adanya permintaan data (*data query*) yang sesuai

dengan kebutuhan pengguna aplikasi. Untuk mengatasi hal ini diperlukan *query* data yang tepat dan sesuai dengan pengguna, yaitu menyaring permintaan data sesuai dengan atribut penanda pengguna, seperti atribut ID pengguna, yang mengakses halaman/fitur tersebut. Selain itu, perlu adanya pemeriksaan pada fitur-situr pada sistem dan menentukan peran/hak akses apa saja kah yang harus dimiliki sebuah pengguna agar dapat mengakses fitur tersebut.

Berkaitan dengan peran/hak akses pengguna, salah satu kasus penggunaan sistem PKK (dapat dilihat pada Gambar 7.1) masih memungkinkan pengguna untuk mengolah data yang semestinya tidak bisa diakses selain pemilik akun PKK wilayahnya, yakni kasus penggunaan “Mengolah data PKK” (kode UC-101). Pada sistem yang ada, seluruh pengguna dapat melakukan aksi menambah, mengubah, dan menghapus data PKK yang ada. Butuh adanya perubahan manajemen pengolahan data PKK agar data yang bisa diolah hanya data PKK milik akun pengguna *login*. Perubahan ini digambarkan pada Gambar 3.2 dan dijelaskan lebih rinci pada Bab 3.5.1.

Selain memastikan penyediaan data yang tepat, untuk menangani kebocoran kerahasiaan data, perlu adanya suatu proses yang memastikan bahwa data-data yang akan disediakan aplikasi adalah benar dimiliki oleh pengguna aplikasi. Data disediakan dalam suatu halaman/fitur aplikasi saat pengguna memuat halaman/jendela tersebut melalui tombol navigasi menuju halaman tersebut atau dengan mengubah *address bar* pada aplikasi *browser*. Oleh karena itu, solusi yang dapat digunakan untuk mengatasi permasalahan ini adalah dengan memanfaatkan perangkat tengah (*middleware*). Proses dan rancangan perubahan ini dijelaskan pada Gambar 3.3, di mana bagian di atas tanda panah merupakan kondisi umum penanganan permintaan (*request*) dari pengguna dan bagian di bawah tanda panah merupakan pemanfaatan perangkat tengah untuk mengatasi permintaan pengguna.

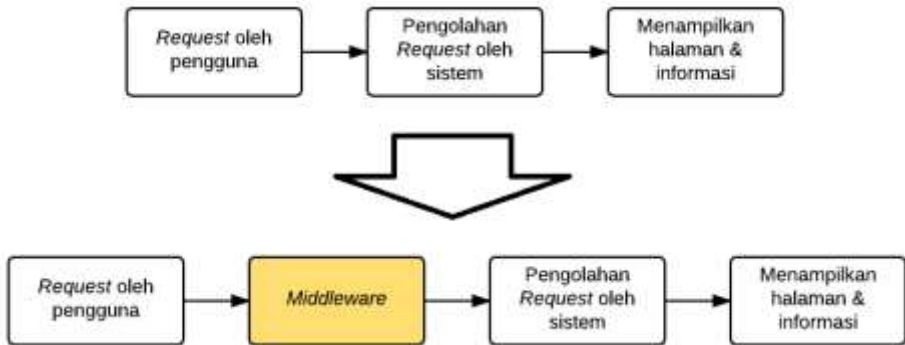


**Gambar 3.2. Penyesuaian Kasus Penggunaan "Mengolah data PKK"**

- *Login*, registrasi pengguna baru, dan mengubah kata sandi

Proses *login*, registrasi pengguna baru, dan mengubah kata sandi melibatkan elemen penting yang dapat menunjukkan atribut unik sebuah pengguna aplikasi, yaitu kata sandi (*password*). Untuk memberikan keamanan informasi akun pengguna perlu adanya enkripsi pada kata sandi pengguna, sehingga pada *request* yang dikirimkan pengguna kepada sistem tidak mengandung nilai kata sandi asli yang dikirimkan oleh pengguna. Penanganan kerahasiaan

kata sandi berbeda antara penanganan pada aplikasi web dan aplikasi perangkat bergerak.



**Gambar 3.3.** Perancangan kerahasiaan data menggunakan *middleware*

Penanganan kerahasiaan kata sandi pada aplikasi web menggunakan metode kriptografi berupa *Hashing*. Metode ini sudah disediakan di dalam kerangka kerja *Laravel* saat pengguna melakukan registrasi (selengkapnya dibahas pada Bab 3.4). *Hashing* merupakan metode kriptografi berupa enkripsi satu arah, di mana hasil enkripsi tidak dapat didekripsi kembali. Metode ini berguna untuk menjaga kerahasiaan data (*confidentiality*) dan memastikan keaslian data (*authentication*) [15].

Penanganan kerahasiaan kata sandi pada aplikasi perangkat bergerak lebih rumit, dikarenakan perbedaan *platform* yang digunakan. Aplikasi perangkat bergerak tidak mendukung fitur otentikasi yang dimiliki aplikasi web karena keterbatasan bahasa pemrograman, di mana aplikasi web menggunakan bahasa PHP dan aplikasi perangkat bergerak menggunakan *JavaScript*. Perbedaan penanganan terletak pada penggunaan metode kriptografi, yaitu penggunaan metode kriptografi yang dapat digunakan pada *JavaScript* karena bahasa PHP bisa mengolah data menggunakan *JavaScript* pada implementasinya. Metode kriptografi untuk penanganan kerahasiaan kata sandi ini menggunakan pustaka

khusus bernama *CryptoJS* yang menggunakan fungsi enkripsi AES.

### 3.4. Perancangan Manajemen Otentisitas Pengguna

Metrik otentisitas pengguna (*authenticity*) pada ISO 25010 melingkupi protokol otentikasi. Protokol otentikasi merupakan proses untuk mengenali pengguna berdasarkan data yang digunakan pengguna saat memasuki sistem (*login*). Agar dapat memasuki sistem, pengguna membutuhkan sepasang data yang menunjukkan keaslian pengguna tersebut. Sepasang data tersebut adalah nama pengguna (*username*) untuk aplikasi web atau nomor HP untuk aplikasi perangkat bergerak dan kata sandi. Diperlukan sebuah proses untuk dapat mengenali sebuah pengguna berdasarkan pasangan data tersebut.

Kerangka kerja *Laravel* menyediakan kelas khusus yang dapat menangani proses otentikasi pengguna yang dinamakan kelas *Auth*. Di dalam kelas ini sudah mencakup fungsi-fungsi *hash* untuk menyimpan dan mengenali kata sandi, memanfaatkan sesi halaman (*page session*) untuk menyaring informasi, dan menyediakan fitur pembagian otorisasi/peran pengguna (*role*). Kelas ini akan menggantikan paket kerangka kerja yang digunakan sebelumnya pada sistem, yaitu *Sentinel 2.0*. Oleh karena itu, dalam protokol otentikasi, penanganannya akan memanfaatkan kelas tersebut karena memiliki proses pengaturan yang mudah meskipun sistem terdiri dari dua buah *platform* yang berbeda.

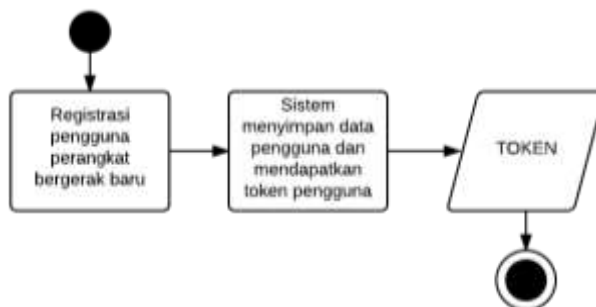
Selain itu, metrik otentisitas pengguna juga melingkupi kesesuaian aturan otentikasi di dalam sistem. Pada aplikasi web, aturan otentikasi akan ditangani menggunakan perangkat tengah (*middleware*) seperti yang ditunjukkan pada Gambar 3.3 sebelumnya. Pada aplikasi perangkat bergerak, dibutuhkan aturan tambahan untuk memastikan bahwa pengguna aplikasi merupakan pengguna asli dari data-data yang akan ditampilkan pada layar perangkat cerdas. Aturan yang akan disediakan adalah verifikasi pengguna perangkat bergerak.

Verifikasi pengguna perangkat bergerak merupakan sebuah proses yang dikembangkan pada Tugas Akhir ini untuk

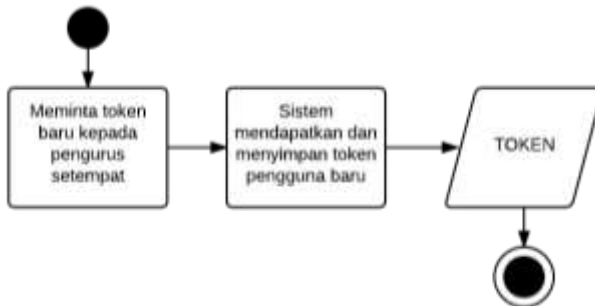
memastikan bahwa pengguna aplikasi perangkat bergerak merupakan pengguna asli data-data yang disediakan aplikasi. Pada saat pengguna melakukan pendaftaran akun pengguna pertama kali, sistem akan menyediakan token pada baris data akun pengguna tersebut dan memberi tanda bahwa pengguna tersebut belum melakukan konfirmasi token. Nilai token berupa serangkaian karakter angka dan huruf yang didapatkan secara acak. Token ini dapat diperoleh oleh pengguna melalui pengurus saat melakukan pendaftaran akun pengguna perangkat bergerak. Pengguna perlu untuk melakukan verifikasi akun dengan memasukkan nilai token tersebut saat melakukan *login* untuk pertama kalinya ke dalam aplikasi pada perangkat yang digunakan (Gambar 3.4). Akan disediakan pula fitur untuk mendapatkan ulang token apabila pengguna kehilangan token saat pendaftaran (Gambar 3.5). Proses verifikasi pengguna perangkat bergerak akan dijelaskan pada Gambar 3.6. Proses verifikasi pengguna perangkat bergerak ini akan dijelaskan lebih lanjut menggunakan diagram kasus penggunaan pada Bab 3.5.1.

### 3.5. Perancangan Fitur Mengenai Kerahasiaan Data dan Otentisitas Pengguna

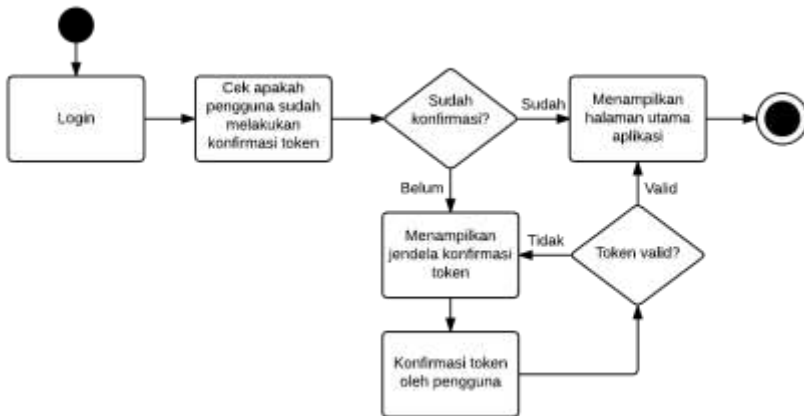
Subbab ini menjelaskan tentang rancangan fitur-fitur tambahan yang berhubungan dengan kerahasiaan data dan otentisitas pengguna dan akan diimplementasikan ke dalam sistem e-PKK *online*. Perancangan fitur-fitur tersebut dijelaskan pada subbab-subbab berikut.



Gambar 3.4. Proses registrasi pengguna perangkat bergerak baru



**Gambar 3.5.** Proses apabila pengguna kehilangan token



**Gambar 3.6.** Proses verifikasi pengguna perangkat bergerak

### 3.5.1. Rancangan Kebutuhan Fungsionalitas

Kebutuhan fungsionalitas yang dimiliki sistem akan dilakukan penambahan berupa fungsionalitas yang dibutuhkan dalam hal manajemen kerahasiaan data dan otentikasi pengguna. Sesuai dengan perancangan yang dijelaskan pada Bab 3.3 maka perlu adanya perubahan kebutuhan fungsionalitas berkaitan dengan pengolahan data PKK dan data Posyandu yang dijelaskan pada Tabel 3.7 dengan kode kebutuhan WPK-061 -063 untuk data PKK dan kode kebutuhan WPO-001-003 untuk data Posyandu.



Kebutuhan fungsionalitas sistem juga bertambah, untuk memenuhi kebutuhan akan aturan otentikasi, yakni registrasi pengguna baru oleh administrator sistem. Pada sistem ini administrator dapat mengolah daftar pengguna sistem. Pengolahan yang dapat dilakukan administrator adalah menambah akun pengguna baru, menghapus akun pengguna, dan *me-reset* kata sandi pengguna. Kebutuhan fungsionalitas terkait *reset* kata sandi dibebankan kepada peran administrator karena proses pendaftaran akun pengurus untuk sistem ini hanya dapat dilakukan melalui administrator sistem sehingga apabila pengguna kehilangan kata sandinya maka pengguna tersebut dapat memperoleh kata sandi baru hanya melalui administrator. Kebutuhan fungsionalitas mengenai registrasi pengguna baru dicantumkan pada Tabel 3.7 dengan kode kebutuhan ADM-001-004. Selengkapnya, kasus penggunaan dan deskripsi mengenai kebutuhan fungsionalitas tersebut akan dijelaskan pada Bab 3.5.2.

Beberapa kebutuhan fungsionalitas lain yang ditambahkan, sesuai dengan kebutuhan kerahasiaan data dan otentikasi pengguna sistem, adalah verifikasi akun oleh pengguna perangkat bergerak (kode kebutuhan MPK-001) dan *reset* token akun pengguna perangkat bergerak oleh pengurus sistem (kode kebutuhan WPK-064 dan WPO-004). Kebutuhan fungsionalitas terkait token akun pengguna perangkat bergerak merupakan kebutuhan untuk memenuhi kebutuhan otentikasi pengguna. Daftar perubahan kebutuhan fungsionalitas pada sistem e-PKK *online* dituliskan pada Tabel 3.7 dan petunjuk penulisan akan dituliskan pada Tabel 3.6. Selengkapnya, kasus penggunaan dan deskripsi mengenai kebutuhan fungsionalitas tersebut akan dijelaskan pada Bab 3.5.2.

**Tabel 3.6. Petunjuk Penulisan Perbandingan Sistem**

Bagian sistem lama (kiri)	Bagian sistem baru (kanan)	Penjelasan
(kosong)	Fitur baru	Penambahan fitur baru
Fitur lama	(kosong)	Fitur lama masih digunakan pada sistem baru
Fitur lama	Fitur baru	Fitur lama dimodifikasi menjadi fitur baru

**Tabel 3.7. Daftar Perbandingan Kebutuhan Fungsionalitas**

Kode	Deskripsi Kebutuhan Sistem Lama	Kode	Deskripsi Kebutuhan Tambahan/Baru
WPK-001	Pengurus PKK dapat login, masuk ke dalam sistem		
WPK-002	Pengurus PKK dapat logout, keluar dari sistem		
WPK-003	Pengurus PKK dapat mengelola data PKK	WPK-061	Pengurus PKK dapat melihat profil akun
WPK-004	Pengurus PKK dapat menambahkan data PKK baru	WPK-062	Pengurus PKK dapat mengubah nama pengguna
WPK-005	Pengurus PKK dapat mengubah data PKK		
WPK-006	Pengurus PKK dapat menghapus data PKK	WPK-063	Pengurus PKK dapat mengubah kata sandi
WPK-007	Pengurus PKK dapat melihat rincian data PKK		
WPK-008	Pengurus PKK dapat mengelola periode kepengurusan PKK		
WPK-009	Pengurus PKK dapat menambahkan periode kepengurusan		
WPK-010	Pengurus PKK dapat mengubah periode kepengurusan		
WPK-011	Pengurus PKK dapat menghapus periode kepengurusan		
WPK-012	Pengurus PKK dapat mengelola jabatan pengurus PKK		

Kode	Deskripsi Kebutuhan Sistem Lama	Kode	Deskripsi Kebutuhan Tambahan/Baru
WPK-013	Pengurus PKK dapat menambahkan jabatan pengurus PKK		
WPK-014	Pengurus PKK dapat mengubah jabatan pengurus PKK		
WPK-015	Pengurus PKK dapat menghapus jabatan pengurus PKK		
WPK-016	Pengurus PKK dapat mengelola pengurus PKK		
WPK-017	Pengurus PKK dapat menambahkan pengurus PKK		
WPK-018	Pengurus PKK dapat mengubah pengurus PKK		
WPK-019	Pengurus PKK dapat menghapus pengurus PKK		
WPK-020	Pengurus PKK dapat mengelola anggota/ibu PKK		
WPK-021	Pengurus PKK dapat menambahkan anggota/ibu PKK		
WPK-022	Pengurus PKK dapat mengubah anggota/ibu PKK		
WPK-023	Pengurus PKK dapat menghapus anggota/ibu PKK		
WPK-024	Pengurus PKK dapat melihat rincian anggota/ibu PKK		
WPK-025	Pengurus PKK dapat mengelola kas PKK		

Kode	Deskripsi Kebutuhan Sistem Lama	Kode	Deskripsi Kebutuhan Tambahan/Baru
WPK-026	Pengurus PKK dapat menambahkan kas PKK		
WPK-027	Pengurus PKK dapat mengubah kas PKK		
WPK-028	Pengurus PKK dapat menghapus kas PKK		
WPK-029	Pengurus PKK dapat mengelola jenis kas PKK		
WPK-030	Pengurus PKK dapat menambahkan jenis kas PKK		
WPK-031	Pengurus PKK dapat mengubah jenis kas PKK		
WPK-032	Pengurus PKK dapat menghapus jenis kas PKK		
WPK-033	Pengurus PKK dapat mengelola absen PKK		
WPK-034	Pengurus PKK dapat menambahkan absen PKK		
WPK-035	Pengurus PKK dapat mengubah absen PKK		
WPK-036	Pengurus PKK dapat menghapus absen PKK		
WPK-037	Pengurus PKK dapat mengelola notulensi PKK		
WPK-038	Pengurus PKK dapat menambahkan notulensi PKK		

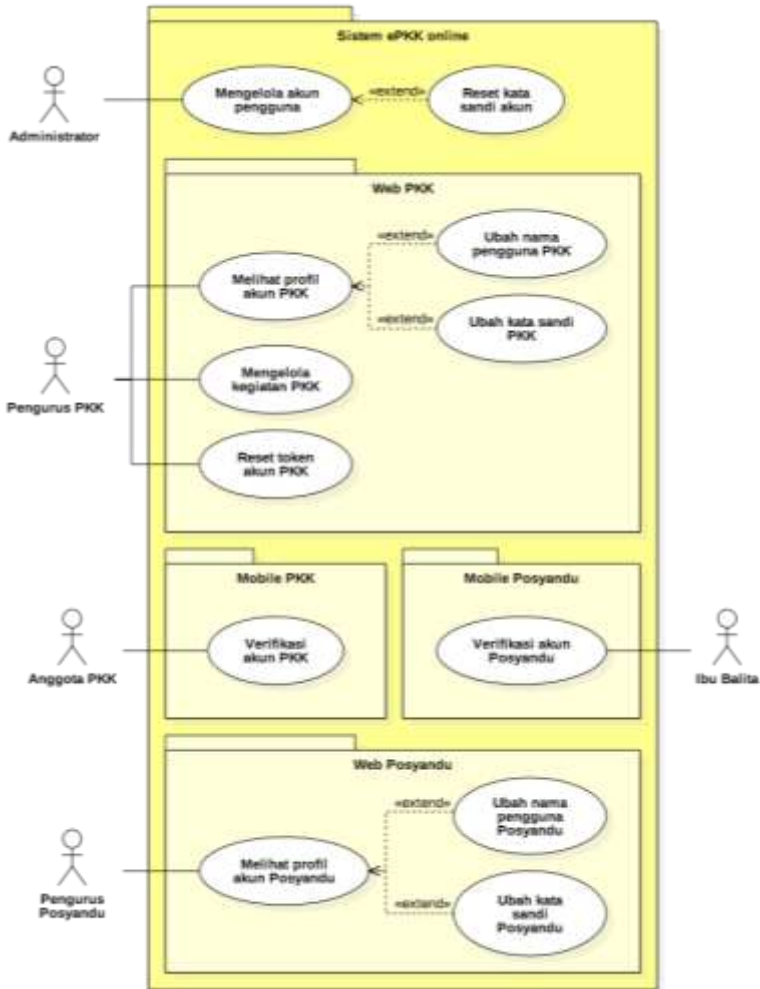
Kode	Deskripsi Kebutuhan Sistem Lama	Kode	Deskripsi Kebutuhan Tambahan/Baru
WPK-039	Pengurus PKK dapat mengubah notulensi PKK		
WPK-040	Pengurus PKK dapat menghapus notulensi PKK		
WPK-041	Pengurus PKK dapat mengelola pengumuman PKK		
WPK-042	Pengurus PKK dapat menambahkan pengumuman PKK		
WPK-043	Pengurus PKK dapat mengubah pengumuman PKK		
WPK-044	Pengurus PKK dapat menghapus pengumuman PKK		
WPK-045	Pengurus PKK dapat melihat rincian pengumuman PKK		
WPK-046	Pengurus PKK dapat mengelola laporan bidang PKK		
WPK-047	Pengurus PKK dapat menambahkan laporan bidang PKK		
WPK-048	Pengurus PKK dapat menghapus laporan bidang PKK		
WPK-049	Pengurus PKK dapat mengunduh laporan bidang PKK		
WPK-050	Pengurus PKK dapat mengelola data jentik nyamuk		

Kode	Deskripsi Kebutuhan Sistem Lama	Kode	Deskripsi Kebutuhan Tambahan/Baru
WPK-051	Pengurus PKK dapat menambah data jentik nyamuk		
WPK-052	Pengurus PKK dapat mengubah data jentik nyamuk		
WPK-053	Pengurus PKK dapat menghapus data jentik nyamuk		
WPK-054	Pengurus PKK dapat menampilkan daftar keluhan		
WPK-055	Pengurus PKK dapat menampilkan rincian keluhan		
WPK-056	Pengurus PKK dapat mengirimkan komentar pada suatu keluhan		
WPK-057	Pengurus PKK dapat mengelola kegiatan PKK		
WPK-058	Pengurus PKK dapat menambah kegiatan		
WPK-059	Pengurus PKK dapat mengubah kegiatan		
WPK-060	Pengurus PKK dapat menghapus kegiatan		
		WPK-064	Pengurus PKK dapat melakukan <i>reset</i> token verifikasi akun pengguna perangkat bergerak
		WPO-001	Pengurus Posyandu dapat melihat profil akun
		WPO-002	Pengurus Posyandu dapat mengubah nama pengguna

Kode	Deskripsi Kebutuhan Sistem Lama	Kode	Deskripsi Kebutuhan Tambahan/Baru
		WPO-003	Pengurus Posyandu dapat mengubah kata sandi
		WPO-004	Pengurus Posyandu dapat melakukan <i>reset</i> token verifikasi akun pengguna perangkat bergerak
		ADM-001	Administrator dapat mengelola akun pengguna
		ADM-002	Administrator dapat menambah akun pengguna baru
		ADM-003	Administrator dapat menghapus akun pengguna
		ADM-004	Administrator dapat melakukan <i>reset</i> kata sandi pengguna
		MPK-001	Anggota PKK dapat melakukan verifikasi akun perangkat bergerak
		MPO-001	Ibu balita dapat melakukan verifikasi akun perangkat bergerak

### 3.5.2. Rancangan Kasus Penggunaan Tambahan Sistem

Subbab ini menjelaskan rancangan implementasi kebutuhan fungsionalitas berupa kasus penggunaan sistem. Rancangan kasus penggunaan dapat dilihat pada Gambar 3.7 dan Tabel 3.8.



Gambar 3.7. Kasus Penggunaan Tambahan Sistem



**Tabel 3.8. Daftar Perbandingan Deskripsi Diagram Kasus Penggunaan**

Kode	Nama Kasus Penggunaan Lama	Kode	Nama Kasus Perubahan Tambahan/Baru	Keterangan
UC-101	Mengelola data PKK	UC-159	Melihat profil akun PKK	Pengguna dapat melihat data mengenai akun PKK yang digunakan
UC-102	Tambah data PKK			
UC-103	Ubah data PKK	UC-160	Ubah nama pengguna PKK	Pengguna dapat mengubah nama pengguna akun PKK
UC-104	Hapus data PKK			
UC-105	Tampilkan rincian data PKK	UC-161	Ubah kata sandi PKK	Pengguna dapat mengubah kata sandi akun PKK
UC-106	Mengelola periode kepengurusan			
UC-107	Tambah periode			
UC-108	Ubah periode			
UC-109	Hapus periode			
UC-110	Mengelola jabatan pengurus			
UC-111	Tambah jabatan			
UC-112	Ubah jabatan			
UC-113	Hapus jabatan			
UC-114	Mengelola pengurus PKK			

Kode	Nama Kasus Penggunaan Lama	Kode	Nama Kasus Perubahan Tambahan/Baru	Keterangan
UC-115	Tambah pengurus			
UC-116	Ubah pengurus			
UC-117	Hapus pengurus			
UC-118	Mengelola anggota PKK			
UC-119	Tambah anggota			
UC-120	Ubah anggota			
UC-121	Hapus anggota			
UC-122	Tampilkan rincian anggota			
UC-123	Mengelola kas PKK			
UC-124	Tambah kas			
UC-125	Ubah kas			
UC-126	Hapus kas			
UC-127	Mengelola jenis kas PKK			
UC-128	Tambah jenis kas			
UC-129	Ubah jenis kas			
UC-130	Hapus jenis kas			
UC-131	Mengelola absen			

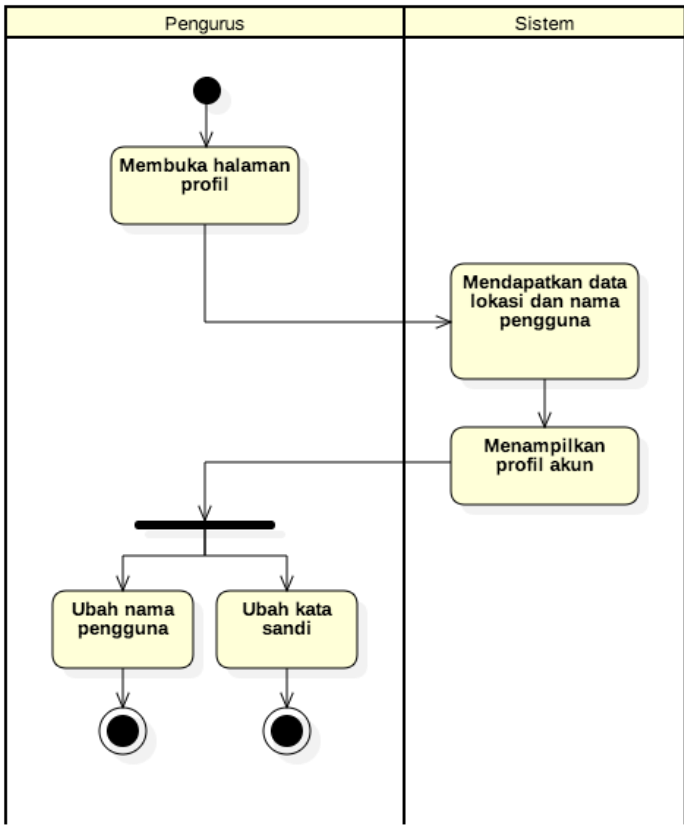
Kode	Nama Kasus Penggunaan Lama	Kode	Nama Kasus Perubahan Tambahan/Baru	Keterangan
UC-132	Tambah absen			
UC-133	Ubah absen			
UC-134	Hapus absen			
UC-135	Mengelola notulensi			
UC-136	Tambah notulensi			
UC-137	Ubah notulensi			
UC-138	Hapus notulensi			
UC-139	Mengelola pengumuman			
UC-140	Tambah pengumuman			
UC-141	Ubah pengumuman			
UC-142	Hapus pengumuman			
UC-143	Melihat rincian pengumuman			
UC-144	Mengelola laporan bidang			
UC-145	Tambah laporan bidang			
UC-146	Hapus laporan bidang			
UC-147	Unduh laporan bidang			

Kode	Nama Kasus Penggunaan Lama	Kode	Nama Kasus Perubahan Tambahan/Baru	Keterangan
UC-148	Mengelola data jentik nyamuk			
UC-149	Tambah data jentik			
UC-150	Ubah data jentik			
UC-151	Hapus data jentik			
UC-152	Menampilkan daftar keluhan			
UC-153	Menampilkan rincian keluhan			
UC-154	Mengirimkan komentar baru			
UC-155	Mengelola kegiatan PKK			
UC-156	Tambah kegiatan			
UC-157	Ubah kegiatan			
UC-158	Hapus kegiatan			
		UC-162	Reset token akun PKK	Pengguna dapat melakukan <i>reset</i> token akun perangkat bergerak PKK
		UC-201	Verifikasi akun PKK	Pengguna dapat melakukan verifikasi akun pengguna perangkat bergerak PKK

Kode	Nama Kasus Penggunaan Lama	Kode	Nama Kasus Perubahan Tambahan/Baru	Keterangan
		UC-301	Melihat profil akun Posyandu	Pengguna dapat melihat data mengenai akun Posyandu yang digunakan
		UC-302	Ubah nama pengguna Posyandu	Pengguna dapat mengubah nama pengguna Posyandu
		UC-303	Ubah kata sandi Posyandu	Pengguna dapat mengubah kata sandi akun Posyandu
		UC-304	<i>Reset</i> token akun Posyandu	Pengguna dapat melakukan <i>reset</i> token akun perangkat bergerak Posyandu
		UC-401	Verifikasi akun Posyandu	Pengguna dapat melakukan verifikasi akun pengguna perangkat bergerak Posyandu
		UC-601	Mengelola akun pengguna	Pengguna dapat mengelola akun pengguna
		UC-602	Tambah akun	Pengguna dapat menambah akun baru
		UC-603	Hapus akun	Pengguna dapat menghapus akun
		UC-604	<i>Reset</i> kata sandi akun	Pengguna dapat melakukan <i>reset</i> kata sandi akun

3.5.2.1. Melihat Profil Akun

Penjelasan mengenai kasus penggunaan “melihat profil akun” akan dijelaskan pada Tabel 3.9. Proses bisnis kasus penggunaan ini akan dijelaskan menggunakan diagram aktivitas seperti pada Gambar 3.8.



Gambar 3.8. Diagram Aktivitas: Melihat Profil Akun

Tabel 3.9. Spesifikasi Kasus Penggunaan: Melihat Profil Akun

Kode Use Case	UC-155 dan UC-301
Nama Use Case	Melihat profil akun PKK/Posyandu

Aktor	Pengurus PKK/Posyandu
Deskripsi	Pengurus dapat melihat data mengenai akun yang digunakan
Kondisi Awal	Pengurus membuka menu profil akun
Kondisi Akhir	Pengurus dapat mengelola data akun: ubah nama pengguna dan kata sandi (UC-156-157 dan UC-302-303)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus membuka menu profil akun	2. Sistem mendapatkan data lokasi wilayah dan nama pengguna yang digunakan 3. Sistem menampilkan profil akun
4. Pengurus dapat melakukan berbagai aksi	
4A. Ubah nama pengguna (UC-156 atau UC-302)	
4B. Ubah kata sandi (UC-157 atau UC-303)	

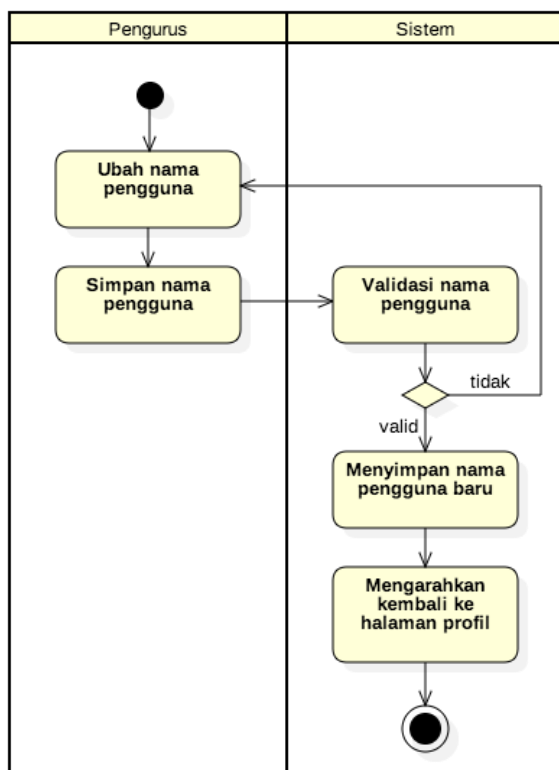
### 3.5.2.2. Ubah Nama Pengguna

Penjelasan mengenai kasus penggunaan “ubah nama pengguna” akan dijelaskan pada Tabel 3.10. Proses bisnis kasus penggunaan ini akan dijelaskan menggunakan diagram aktivitas seperti pada Gambar 3.9.

**Tabel 3.10. Spesifikasi Kasus Penggunaan: Ubah Nama Pengguna**

Kode Use Case	UC-156 dan UC-302
Nama Use Case	Ubah nama pengguna PKK/Posyandu
Aktor	Pengurus PKK/Posyandu
Deskripsi	Pengurus dapat mengubah nama pengguna akun
Kondisi Awal	Pengurus berada pada halaman profil akun
Kondisi Akhir	Pengurus memiliki nama pengguna baru
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus mengubah nama pengguna	
2. Pengurus menyimpan nama pengguna	

	3. Sistem melakukan validasi nama pengguna 3A. Nama pengguna tidak valid 4. Sistem menyimpan nama pengguna baru 5. Sistem mengarahkan kembali pengguna menuju halaman profil
Alur Kejadian Alternatif	
	3A. Nama pengguna tidak valid Sistem mengarahkan pengguna kembali menuju halaman profil dengan notifikasi kegagalan penyimpanan nama pengguna baru

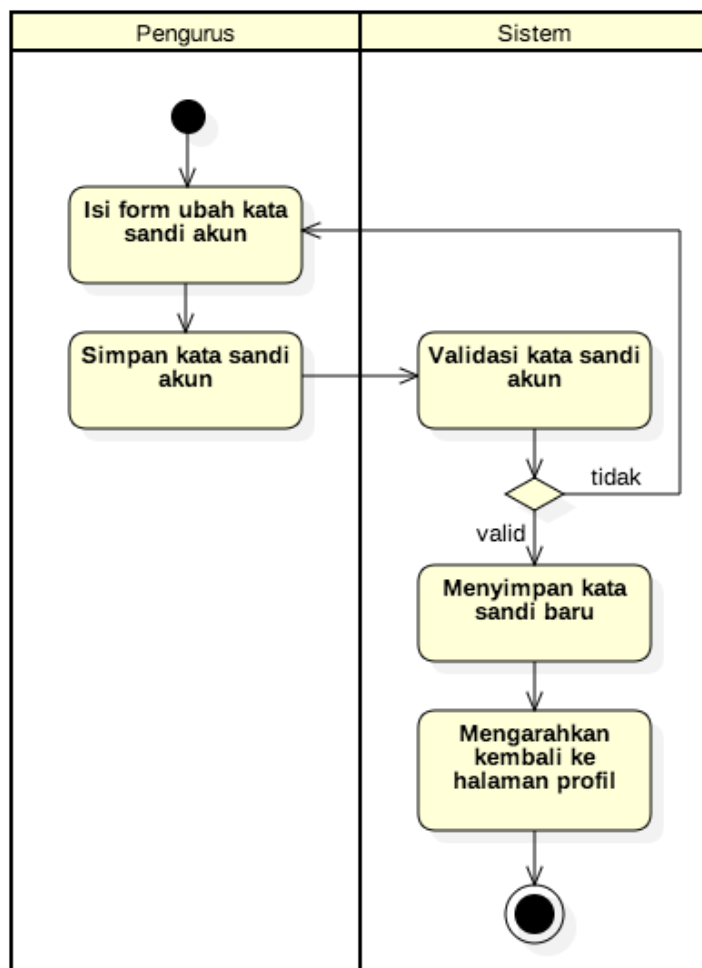


Gambar 3.9. Diagram Aktivitas: Ubah Nama Pengguna



### 3.5.2.3. Ubah Kata Sandi

Penjelasan mengenai kasus penggunaan “ubah kata sandi” akan dijelaskan pada Tabel 3.11. Proses bisnis kasus penggunaan ini akan dijelaskan menggunakan diagram aktivitas seperti pada Gambar 3.10.



Gambar 3.10. Diagram Aktivitas: Ubah Kata Sandi

**Tabel 3.11. Spesifikasi Kasus Penggunaan: Ubah Kata Sandi**

Kode Use Case	UC-157 dan UC-303		
Nama Use Case	Ubah kata sandi PKK/Posyandu		
Aktor	Pengurus PKK/Posyandu		
Deskripsi	Pengurus dapat mengubah kata sandi akun		
Kondisi Awal	Pengurus berada pada halaman profil akun		
Kondisi Akhir	Pengurus memiliki kata sandi baru		
Alur Kejadian Normal			
Aktor		Sistem	
1. Pengurus mengisi <i>form</i> kata sandi 2. Pengurus menyimpan kata sandi		3. Sistem melakukan validasi kata sandi 3A. Kata sandi tidak valid 4. Sistem menyimpan kata sandi baru 5. Sistem mengarahkan kembali pengguna menuju halaman profil	
Alur Kejadian Alternatif			
		3A. Kata sandi tidak valid Sistem mengarahkan pengguna kembali menuju halaman profil dengan notifikasi kegagalan penyimpanan kata sandi baru	

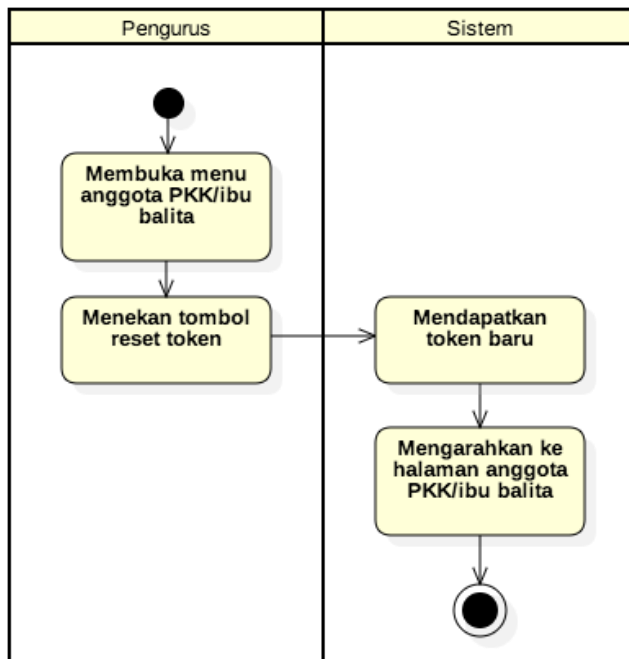
#### 3.5.2.4. *Reset Token Akun*

Penjelasan mengenai kasus penggunaan “*reset token akun*” akan dijelaskan pada Tabel 3.12. Proses bisnis kasus penggunaan ini akan dijelaskan menggunakan diagram aktivitas seperti pada Gambar 3.11.

**Tabel 3.12. Spesifikasi Kasus Penggunaan: *Reset Token Akun***

Kode Use Case	UC-162 dan UC-304
Nama Use Case	Reset token akun PKK/Posyandu
Aktor	Pengurus PKK/Posyandu
Deskripsi	Pengguna dapat melakukan <i>reset</i> token akun perangkat bergerak
Kondisi Awal	Pengurus membuka menu anggota PKK/ibu balita
Kondisi Akhir	Pengurus mendapatkan token akun perangkat bergerak baru
Alur Kejadian Normal	

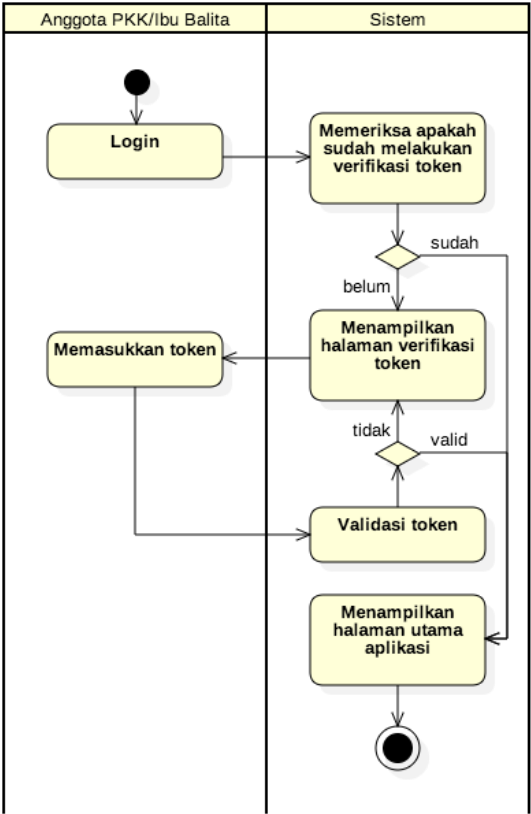
Aktor	Sistem
1. Pengurus membuka menu anggota PKK/ibu balita 2. Pengurus menekan tombol <i>reset</i> token untuk akun pilihan	3. Sistem mendapatkan token baru 4. Sistem mengarahkan pengguna kembali ke halaman anggota PKK/ibu balita dengan menampilkan token baru



Gambar 3.11. Diagram Aktivitas: *Reset Token Akun*

### 3.5.2.1. Verifikasi Akun

Penjelasan mengenai kasus penggunaan “verifikasi akun” akan dijelaskan pada Tabel 3.13. Proses bisnis kasus penggunaan ini akan dijelaskan menggunakan diagram aktivitas seperti pada Gambar 3.12.



Gambar 3.12. Diagram Aktivitas: Verifikasi Akun

Tabel 3.13. Spesifikasi Kasus Penggunaan: Verifikasi Akun

Kode Use Case	UC-201 dan UC-401	
Nama Use Case	Verifikasi akun PKK/Posyandu	
Aktor	Anggota PKK/ibu balita	
Deskripsi	Pengguna dapat melakukan verifikasi akun pengguna perangkat bergerak	
Kondisi Awal	Pengguna melakukan <i>login</i>	
Kondisi Akhir	Akun pengguna sudah terverifikasi	
Alur Kejadian Normal		
Aktor		Sistem

1. Pengguna melakukan <i>login</i>	2. Sistem memeriksa apakah sudah melakukan verifikasi token pada perangkat yang digunakan 2A. Sudah terverifikasi
4. Pengguna memasukkan token	3. Sistem menampilkan halaman verifikasi token 5. Sistem melakukan validasi token 5A. Token tidak valid 6. Sistem menampilkan halaman utama aplikasi
Alur Kejadian Alternatif	
	2A. Sudah terverifikasi Langsung menuju alur nomor 6  5A. Token tidak valid Pengguna diarahkan kembali menuju halaman verifikasi token

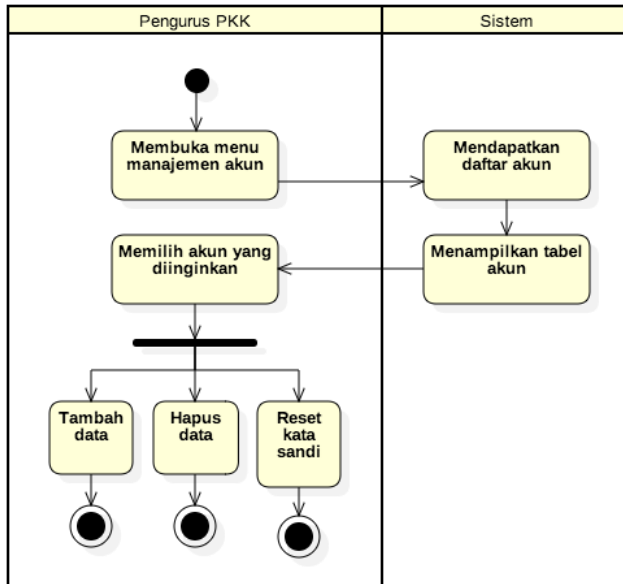
### 3.5.2.2. Mengelola Akun Pengguna

Penjelasan mengenai kasus penggunaan “mengelola akun pengguna” akan dijelaskan pada Tabel 3.14. Proses bisnis kasus penggunaan ini akan dijelaskan menggunakan diagram aktivitas seperti pada Gambar 3.13.

**Tabel 3.14. Spesifikasi Kasus Penggunaan: Mengelola Akun Pengguna**

Kode Use Case	UC-601
Nama Use Case	Mengelola akun pengguna
Aktor	Administrator
Deskripsi	Administrator dapat mengelola akun pengguna
Kondisi Awal	Administrator membuka menu
Kondisi Akhir	Administrator dapat mengelola data akun: tambah akun, hapus akun, dan <i>reset</i> kata sandi (UC-602-604)
Alur Kejadian Normal	
Aktor	Sistem
1. Administrator membuka menu manajemen akun pengguna	2. Sistem mendapatkan daftar akun 3. Sistem menampilkan daftar akun

4. Administrator memilih akun yang diinginkan 5. Administrator dapat melakukan: 5A. Tambah akun (UC-602) 5B. Hapus akun (UC-603) 5C. <i>Reset</i> kata sandi akun (UC-604)	
--	--

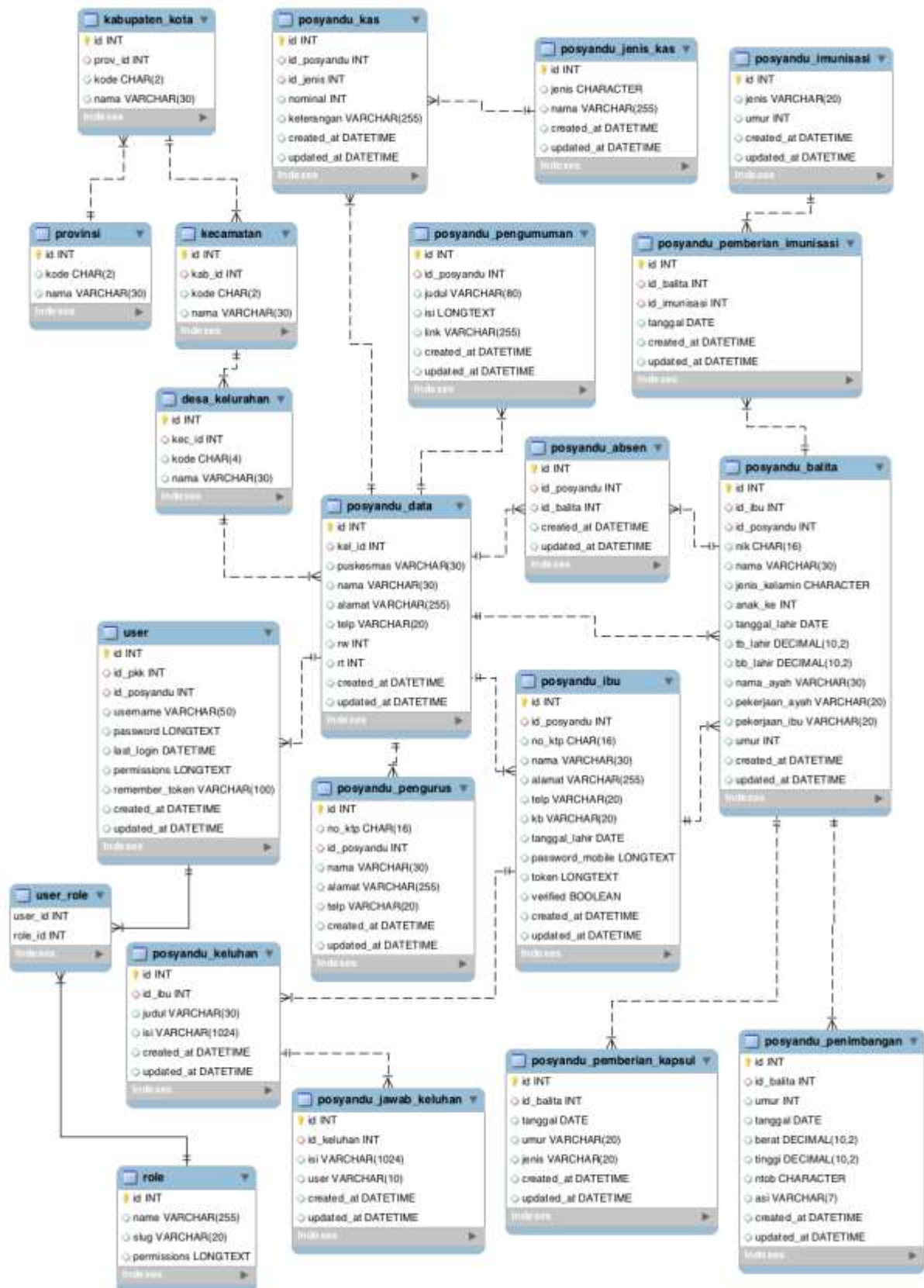


Gambar 3.13. Diagram Aktivitas: Mengelola Akun Pengguna

### 3.5.3. Rancangan Basis Data

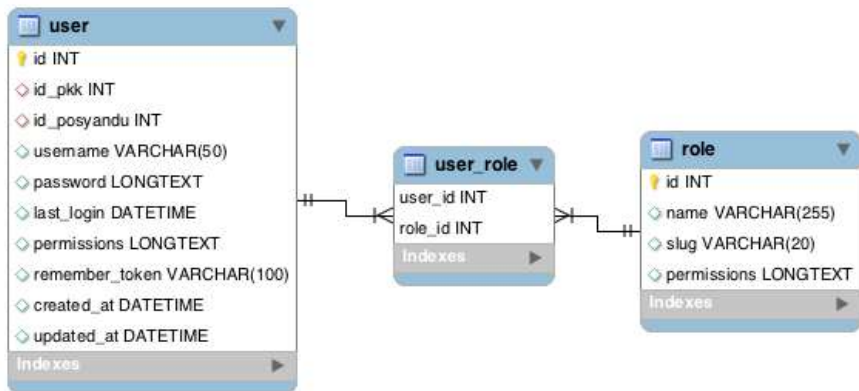
Basis data sistem yang dimodifikasi dibagi menjadi 3 (tiga) bagian, yaitu sistem PKK, sistem Posyandu, dan bagian penghubung (lokasi dan pengaturan pengguna). Bagian penghubung terdiri dari tabel lokasi dan tabel manajemen pengguna. Basis data bagian penghubung dapat dilihat pada Gambar 3.16 dan Gambar 3.17. PDM sistem PKK berisikan tabel-tabel pendukung sistem PKK dan dapat dilihat pada Gambar 3.14. PDM sistem Posyandu berisikan tabel-tabel pendukung kinerja sistem Posyandu dan dapat dilihat pada Gambar 3.15.



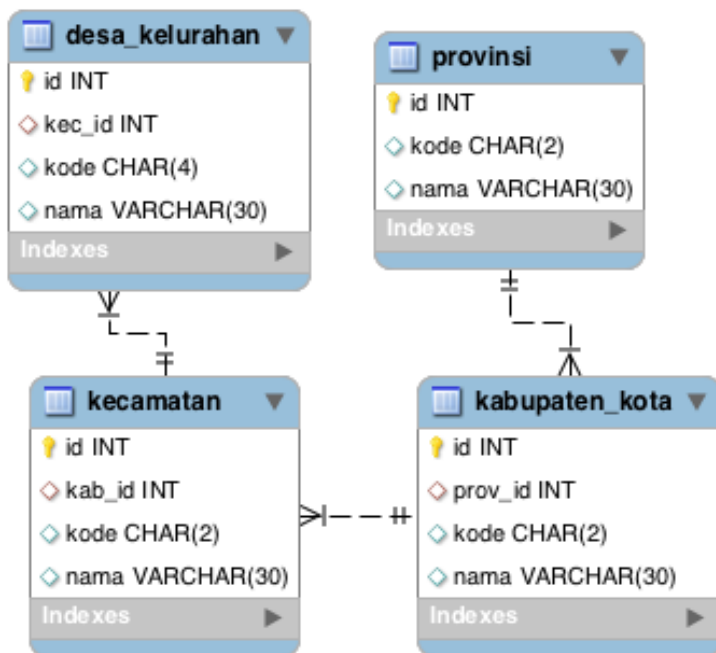


Gambar 3.15. PDM Perubahan Sistem Posyandu





**Gambar 3.16. PDM bagian penghubung (manajemen pengguna) sistem e-PKK online**



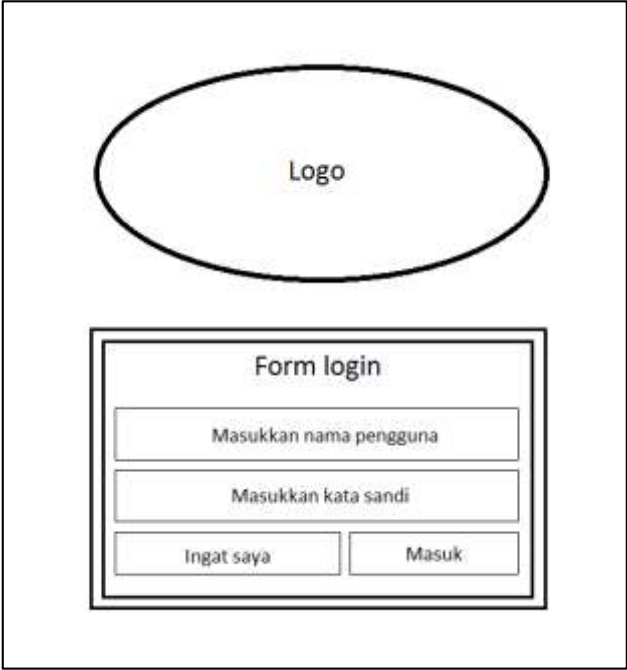
**Gambar 3.17. PDM bagian penghubung (lokasi) sistem e-PKK online**

### 3.6. Perancangan Antarmuka Pengguna

Subbab ini membahas rancangan tampilan antarmuka pada sistem yang diajukan untuk menyesuaikan tingkat kualitas sistem seperti yang diajukan pada subbab-subbab sebelumnya. Terdapat 3 jenis tampilan yang dijelaskan pada subbab-subbab berikut.

#### 3.6.1. Rancangan Antarmuka Halaman Login

Halaman ini merupakan tampilan awal ketika pengguna memasuki sistem karena aplikasi web ini hanya dapat diakses oleh pengurus yang terdaftar. Halaman ini dapat dibagi menjadi 3 (tiga) bagian, yaitu bagian logo dan bagian *form login*. Pada bagian logo akan terdapat logo sistem terkait. Pada bagian *form login* akan terdapat kolom nama user, kolom kata sandi, *checkbox* fitur ingat saya, dan tombol masuk. Rancangan antarmuka pada halaman ini dapat dilihat pada Gambar 3.18.



The diagram illustrates the layout of a login page. At the top, there is a large oval shape labeled "Logo". Below the logo, there is a rectangular box titled "Form login". Inside this box, there are two input fields: the first is labeled "Masukkan nama pengguna" and the second is labeled "Masukkan kata sandi". Below these fields, there are two buttons: "Ingat saya" (Remember me) and "Masuk" (Login).

Gambar 3.18. Rancangan Antarmuka Halaman Login

### 3.6.2. Rancangan Antarmuka Halaman Verifikasi Akun

Halaman ini merupakan tampilan setelah pengguna melakukan *login* untuk pertama kalinya pada sebuah perangkat bergerak. Pada halaman ini terdapat judul halaman, sebuah kolom teks, dan sebuah tombol. Elemen judul halaman digunakan untuk menunjukkan halaman apa yang sedang aktif, untuk hal ini adalah halaman verifikasi akun perangkat bergerak. Kolom teks digunakan untuk memasukkan token yang diperoleh dari pengurus. Tombol yang disediakan adalah tombol untuk mengirimkan token untuk divalidasi oleh sistem. Rancangan antarmuka pada halaman ini dapat dilihat pada Gambar 3.19.



VERIFIKASI AKUN

Masukkan token akun

Selesai

Gambar 3.19. Rancangan Antarmuka Halaman Verifikasi Akun Perangkat Bergerak

Nama Sistem				
<div>Sidebar</div>	Header halaman			
	<div>Bagian profil</div> <div>Kode Wilayah</div> <div>Daerah</div> <div>Provinsi</div> <div>Kabupaten/Kota</div> <div>Kecamatan</div> <div>Desa/Kelurahan</div> <div>RW</div> <div>RT</div>	<div>Bagian nama pengguna</div> <div>Kolom nama pengguna</div> <div>Simpan</div>		
			<div>Bagian manajemen kata sandi</div> <div>Kolom kata sandi lama</div> <div>Kolom kata sandi baru</div> <div>Kolom konfirmasi kata sandi baru</div> <div>Simpan</div>	

Gambar 3.20. Rancangan Antarmuka Halaman Profil Akun

### **3.6.3. Rancangan Antarmuka Halaman Lihat Profil Akun**

Halaman ini merupakan tampilan ketika pengguna menekan menu profil akun pada bagian *sidebar* setelah sudah melakukan *login*. Halaman ini dapat dibagi menjadi 3 (tiga) bagian, yaitu bagian profil, bagian nama pengguna, bagian manajemen kata sandi akun. Pada bagian profil akan ditampilkan wilayah naungan pengguna yang *login*. Pada bagian nama pengguna terdapat kolom nama pengguna yang otomatis berisikan nama pengguna yang digunakan untuk *login* dan tombol simpan. Pada bagian manajemen kata sandi terdapat kolom kata sandi lama, kata sandi baru, konfirmasi kata sandi baru, dan tombol simpan kata sandi baru. Bagian manajemen kata sandi ini digunakan untuk mengubah kata sandi akun pengguna. Rancangan antarmuka pada halaman ini dapat dilihat pada Gambar 3.20.

*[Halaman ini sengaja dikosongkan]*

## **BAB IV IMPLEMENTASI**

Bab ini membahas implementasi dari perancangan aplikasi. Implementasi yang dijelaskan meliputi lingkungan implementasi, implementasi proses-proses yang terjadi di dalam sistem, dan implementasi antarmuka.

### **4.1. Lingkungan Implementasi**

Lingkungan implementasi sistem yang digunakan untuk mengembangkan Tugas Akhir memiliki spesifikasi perangkat keras dan perangkat lunak seperti yang ditampilkan pada Tabel 4.1.

**Tabel 4.1. Lingkungan Implementasi Sistem**

Perangkat	Spesifikasi
Perangkat keras	Prosesor: 1.86 GHz Intel® Core™ 2 Duo Memori: 2.00 GB 1067 MHz DDR3
Perangkat lunak	Sistem Operasi: OS X El Capitan Versi 10.11.5 Bahasa Pemrograman: HTML5, PHP, SQL, JavaScript Kerangka Kerja: Laravel 5.1, PhoneGap Kakas Pembantu: StarUML, PowerDesigner, Sublime Text 3, MAMP

### **4.2. Implementasi Proses**

Subbab ini menjelaskan tentang implementasi proses-proses yang terjadi di dalam sistem. Beberapa implementasi proses yang diimplementasikan akan diterangkan pada subbab-subbab berikut.

#### **4.2.1. Implementasi Konfigurasi Otentikasi *Laravel 5.1***

Subbab ini membahas konfigurasi/pengaturan agar sistem dapat menggunakan fitur otentikasi yang disediakan kerangka kerja *Laravel* versi 5.1. Pada halaman utama *Laravel 5.1* sudah dijelaskan pengaturan umum agar pengembang dapat memanfaatkan fitur ini [10], tetapi perlu adanya penyesuaian agar fitur ini dapat digunakan pada sistem e-PKK *online*. Beberapa file

yang perlu dilakukan perubahan pada implementasi konfigurasi ini adalah sebagai berikut:

- **app/User.php**: dokumen model data pengguna
- **config/auth.php**: dokumen konfigurasi otentikasi *Laravel*
- **database/migrations/2016\_03\_26\_172319\_create\_general\_tables.php**: dokumen migrasi berisikan skema pembuatan tabel pengguna

Pada dokumen model pengguna perlu dilakukan penambahan pustaka/kelas yang mendukung proses otentikasi yang disediakan *Laravel 5.1*. Implementasi pada dokumen ini dapat dilihat pada Kode Sumber 4.1 dengan catatan bahwa tulisan dengan arsiran berwarna kuning merupakan implementasi konfigurasi.

```

1  <?php
2
3  namespace App;
4
5  use App\Date;
6
7  use Illuminate\Auth\Authenticatable;
8  use Illuminate\Database\Eloquent\Model;
9  use Illuminate\Auth\Passwords\CanResetPassword;
10 use Illuminate\Contracts\Auth\Authenticatable as
    AuthenticatableContract;
11 use Illuminate\Contracts\Auth\CanResetPassword as
    CanResetPasswordContract;
12
13 class User extends Model implements
    AuthenticatableContract, CanResetPasswordContract
14 {
15     use Authenticatable, CanResetPassword;
16     protected $table = 'user';
17
18     protected $fillable = [
19         'id_pkk', 'id_Posyandu', 'username',
20         'last_login', 'permissions',
21     ]
22     protected $hidden = [
23         'password', 'remember_token'
24     ]
25     ...
26 }
```

**Kode Sumber 4.1. Konfigurasi Otentikasi *Laravel* pada dokumen **app/User.php****



Pada dokumen konfigurasi otentikasi utama *Laravel 5.1* perlu ditambahkan perubahan agar tabel pengguna digunakan sebagai tabel utama dalam proses otentikasi. Implementasi pada dokumen ini dapat dilihat pada Kode Sumber 4.2 dengan catatan tulisan dengan arsiran kuning merupakan implementasi konfigurasi.

```

1  <?php
2      ...
3      /*
4      |-----
5      | Authentication Table
6      |-----
7      | ...
8      */
9      'table' => 'user'
10     ...

```

**Kode Sumber 4.2. Konfigurasi Otentikasi *Laravel* pada dokumen config/auth.php**

Pada dokumen migrasi perlu dilakukan penambahan baris kode agar tabel pengguna memiliki atribut yang menampung token “ingat saya” berisikan serangkaian karakter. Implementasi pada dokumen ini dapat dilihat pada Kode Sumber 4.3 dengan catatan bahwa tulisan dengan arsiran berwarna kuning merupakan implementasi konfigurasi.

```

1  <?php
2      ...
18     Schema::create( 'user', function ( Blueprint $table
19     ) {
20         $table->increments( 'id' );
21         $table->integer( 'id_pkk' )->unsigned();
22         $table->integer( 'id_Posyandu' )->unsigned();
23         $table->string( 'username', 50 );
24         $table->text( 'password' );
25         $table->timestamp( 'last_login' );
26         $table->text( 'permissions' );
27         $table->rememberToken();
28         $table->timestamps();
29
30         $table->unique( 'username' );
31     } );
32     ...

```

**Kode Sumber 4.3. Konfigurasi Otentikasi *Laravel* pada dokumen database/migrations/2016\_03\_26\_172319\_create\_general\_tables.php**

#### 4.2.2. Implementasi Perangkat Tengah (*Middleware*)

Perangkat tengah (*middleware*) pada sistem ini berfungsi sebagai layanan penentu apakah pengguna yang mengakses suatu jalur (*route*)/halaman memiliki hak untuk mengakses. Keluaran dari proses yang dialami perangkat ini dapat dibagi menjadi 2 (dua), yaitu pengguna memiliki hak atau pengguna tidak memiliki hak. Pengguna yang memiliki hak akan diarahkan menuju jalur/halaman terkait dan disajikan data-data yang disediakan halaman tersebut. Pengguna yang tidak memiliki hak akses akan diarahkan menuju halaman lain untuk menanggulangi pengguna tersebut mengakses jalur/halaman yang tidak bukan haknya. Perangkat tengah diimplementasikan dalam sistem e-PKK *online* pada aplikasi web dengan pengelompokan per halaman dan dapat dilihat pada Tabel 4.2. Jalur/halaman yang tidak tertulis pada tabel tersebut menandakan bahwa jalur/halaman tersebut dapat diakses tanpa hak akses tertentu.

**Tabel 4.2. Daftar Implementasi Perangkat Tengah**

Halaman	Jalur	<i>Middleware</i>
Profil akun PKK	pkk/profile	pkk-login (PkkLoginMiddleware.php)
Anggota PKK	pkk/ibu	
Jenis Kas PKK	pkk/jeniskas	
Kas PKK	pkk/kas	
Periode kepengurusan PKK	pkk/periode	
Jabatan kepengurusan PKK	pkk/jabatan	
Pengurus PKK	pkk/pengurus	
Kegiatan PKK	pkk/kegiatan	
Notulensi kegiatan PKK	pkk/notulensi	
Jentik Nyamuk	pkk/jentik	
Pengumuman PKK	pkk/pengumuman	
Laporan Bidang PKK	pkk/laporan	
Keluhan PKK	pkk/keluhan	Posyandu-login (PosyanduLoginMiddleware.php)
Profil akun Posyandu	posyandu/profile	
Data balita	posyandu/balita	
Data ibu balita	posyandu/ibu	
Penimbangan balita	posyandu/penimbangan	
Pemberian imunisasi	posyandu/beriimunisasi	
Pemberian kapsul	posyandu/kapsul	

Pengurus Posyandu	posyandu/pengurus	pkk-admin-login (PkkAdminLogi nMiddleware. php)
Kas Posyandu	posyandu/kas	
Absen balita	posyandu/absen	
Keluhan Posyandu	posyandu/keluhan	
Administrator PKK	pkk-admin	
Manajemen akun pengguna PKK	pkk-admin/profile	posyandu-admin- login (PosyanduAdmi nLoginMiddle ware.php)
Administrator Posyandu	posyandu-admin	
Manajemen akun pengguna Posyandu	posyandu- admin/profile	
Manajemen akun pengguna Posyandu per lokasi	posyandu/admin/ [provinsi/kabupaten/ kecamatan/kelurahan]	
Manajemen data jenis imunisasi Posyandu	posyandu/admin/ jenisimunisasi	

#### 4.2.3. Implementasi Pengolahan Kata Sandi Akun Perangkat Bergerak

Proses registrasi akun baru untuk pengguna perangkat bergerak dilakukan pada aplikasi web, baik sistem PKK maupun sistem Posyandu. Proses ini perlu adanya dikarenakan algoritma yang digunakan tiap kerangka kerja, pada web dan perangkat bergerak, adalah berbeda. Maka dari itu, perlu adanya penyimpanan kata sandi dengan metode yang sama dengan metode perangkat bergerak agar kata sandi yang sudah dienkripsi dapat dibaca pada aplikasi manapun.

Pengolahan kata sandi untuk akun perangkat bergerak memerlukan pustaka khusus bernama *CryptoJS* berisikan algoritma AES dan dimodifikasi sedemikian rupa sehingga algoritma AES *CryptoJS* dapat digunakan pada bahasa *JavaScript* maupun PHP. Proses enkripsi dilakukan saat pengguna melakukan *submit*, yaitu menekan tombol simpan. Sebelum data dikirimkan ke *server*, isi dari kolom kata sandi, beserta konfirmasinya, akan dienkripsi terlebih dahulu. Implementasi penggunaan pustaka ini pada penyimpanan kata sandi akun perangkat bergerak dapat dilihat pada Kode Sumber 4.4.

```

1  {!! HTML::script( 'js/aes.js' ) !!}
2  {!! HTML::script( 'js/aes-json-format.js' ) !!}
3  <script type="text/javascript">
4      $( function() {
5          $( 'form' ).bind( 'submit', function() {
6              if ( "input[name=password_mobile]" [0].value
7              != "" ) {
8                  $( "input[name=password_mobile]" [0].value =
9                  CryptoJs.AES.encrypt( JSON.stringify( $(
10                 "input[name=password_mobile]" [0].value ),
11                 "sistemPKK", { format: CryptoJSAesJson }
12                 ).toString();
13             }
14         } );
15     } );
16 </script>

```

**Kode Sumber 4.4. Implementasi Enkripsi AES *CryptoJS* pada Penyimpanan Kata Sandi Akun Perangkat Bergerak**

Baris ke-1 pada Kode Sumber 4.4 merupakan kode program menggunakan sintaks *Blade* milik *Laravel* untuk menggunakan pustaka AES *CryptoJS*. Baris ke-2 merupakan modifikasi agar algoritma AES *CryptoJS* diolah dalam format *CryptoJSAesJson*, menggunakan dasar format JSON (*JavaScript Object Notation*) [16], sehingga dapat digunakan pada *platform* manapun, baik web maupun perangkat bergerak. Enkripsi AES *CryptoJS* akan menghasilkan data dalam format JSON berisikan 3 (tiga) buah kunci, yaitu *ct* (*ciphertext* – kata sandi), *iv* (nilai IV algoritma AES), dan *s* (*salt* – nilai pembeda). Baris ke-7 dan ke-8 merupakan implementasi penggunaan AES *CryptoJS*.

Pengolahan kata sandi juga dilakukan pada pihak penyaji (*server*), yang menggunakan bahasa PHP, berupa proses dekripsi kata sandi. Salah satu penggunaan metode dekripsi AES *CryptoJS* adalah pada saat proses *login* pada aplikasi perangkat bergerak. *Server* akan memeriksa data yang dikirimkan aplikasi perangkat bergerak, yaitu nomor telepon dan kata sandi. Kata sandi yang dikirimkan dalam format enkripsi AES *CryptoJS* dan perlu untuk didekripsi untuk mencocokkan apakah akun menggunakan nomor telepon tersebut memiliki kata sandi yang sama. Implementasi proses dekripsi pada *server* dapat dilihat pada Kode Sumber 4.5.

```

1  public function login()
2  {
3      $data = Input::all();
4
5      $ibu = PkkIbu::where( 'telp', $data['telp'] )->first();
6      if ( $ibu ) {
7          $db = Cryptography::cryptoJsAesDecrypt(
8              "sistemPkk", $ibu->password_mobile );
9          $send = Cryptography::cryptoJsAesDecrypt(
10             "sistemPkk", $data['pass'] );
11
12         if ( $db == $send ) {
13             ...
14         }
15     }

```

**Kode Sumber 4.5. Implementasi Dekripsi AES *CryptoJS* pada Proses Login Aplikasi Perangkat Bergerak**

Implementasi algoritma AES *CryptoJS* pada pihak penyedia diletakkan pada sebuah kelas bernama *Cryptography*. Di dalam kelas ini berisikan algoritma enkripsi dan dekripsi untuk mengolah data agar dapat diolah pula oleh pustaka *CryptoJS* menggunakan bahasa *JavaScript*. Penggunaan kelas ini ditunjukkan pada baris ke-7 dan ke-8 pada Kode Sumber 4.5. Kedua baris tersebut menunjukkan proses dekripsi AES *CryptoJS* untuk kata sandi pengguna yang berada di basis data dan kata sandi yang dikirimkan dari aplikasi perangkat bergerak, dan kemudian dilakukan perbandingan hasil dekripsi (baris ke-10). Apabila hasil dekripsi menunjukkan nilai sama maka kata sandi yang digunakan saat *login* adalah benar dan pengguna dapat memasuki sistem.

#### 4.2.4. Implementasi Algoritma Mendapatkan Token

Token yang digunakan pada sistem ini adalah 8 (delapan) buah rangkaian karakter yang terdiri dari angka dan huruf kapital dan didapatkan secara acak. Token ini digunakan sebagai implementasi metrik otentisitas pengguna dalam komunikasi aplikasi perangkat bergerak dan aplikasi web di dalam tiap sub-sistem e-PKK *online*. Proses mendapatkan token ditunjukkan pada Kode Sumber 4.6.

```

1 public function generateToken()
2 {
3     $chars = "1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ";
4     $token = "";
5     for ( $i = 0; $i < 8; $i++ ) {
6         $token .= $chars[rand( 0, strlen( $chars ) )];
7     }
8     return $token;
9 }

```

**Kode Sumber 4.6. Implementasi Algoritma Mendapatkan Token**

#### 4.2.5. Implementasi Pengecekan Konfirmasi Token Akun

Proses pengecekan token akun dimulai setelah pengguna perangkat bergerak melakukan *login*. Aplikasi mengirimkan data nomor telepon dan kata sandi, yang dibutuhkan pada proses *login*, serta mengirimkan nilai token yang disimpan pada memori lokal aplikasi. Data yang dikirimkan aplikasi akan diolah oleh *server* untuk menentukan apakah proses *login* berhasil dan apakah token sudah pernah dimasukkan dan cocok. Proses pengecekan apakah pengguna sudah pernah melakukan konfirmasi token ditunjukkan pada Kode Sumber 4.7.

```

1 function isUserExist() {
2     if ( $('#login-telp').val().length > 0 && $('#login-
3         password').val().length > 0 ) {
4         $.ajax( {
5             dataType: "json",
6             url: url + "/login",
7             data: {
8                 telp: $('#login-telp').val(),
9                 pass: CryptoJS.AES.encrypt( JSON.stringify(
10                    $('#login-password').val() ), "sistemPKK", { format:
11                    CryptoJS.AesJson } ).toString(),
12                 token: window.localStorage.getItem( "token" )
13             },
14             success: function( result ) {
15                 if ( result.status == "SUCCESS" ) {
16                     sessionStorage.userid = result.id;
17                     if ( result.token == "VERIFIED" ) {
18                         $.mobile.changePage("#main");
19                     }
20                     else {
21                         $.mobile.chamgePage("#token");
22                     }
23                 }
24             }
25         }
26     }
27     else {

```

```

22      $('#login-fail').popup("open");
23    }
24    $('#login-form')[0].reset();
25  },
26  error: function( jqXHR, exception ) {
27    alert( jqXHR.status + " : " + exception );
28  }
29  } );
30 }
31 else {
32   $('#login-emptyfield').popup("open");
33 }
34 }

```

**Kode Sumber 4.7. Implementasi Proses Pengecekan Konfirmasi Token Pengguna Perangkat Bergerak**

Kode Sumber 4.7 menunjukkan proses pengecekan apakah aplikasi pada suatu perangkat bergerak sudah pernah dilakukan proses konfirmasi token, yang juga dilakukan pada saat proses *login*. Proses komunikasi antara aplikasi perangkat bergerak dan aplikasi web menggunakan proses AJAX, digunakan pada baris ke-3. Baris ke-9 menunjukkan bahwa token yang disimpan pada memori local aplikasi diikutsertakan untuk dikirimkan dan diolah oleh *server*. Baris ke-14 merupakan penentu kondisi apakah token yang dikirimkan sesuai dengan token yang ada di *server* dan pengguna langsung diarahkan menuju halaman utama aplikasi (baris ke-15). Apabila token tidak sesuai maka pengguna akan diarahkan menuju halaman konfirmasi token (baris ke-18). Proses pemeriksaan kesesuaian token ditunjukkan pada Kode Sumber 4.8.

```

1  public function verifyToken()
2  {
3    $data = Input::all();
4
5    $ibu = PkkIbu::find( $data['session'] );
6    if ( $ibu ) {
7      $db = Cryptography::cryptoJsAesDecrypt (
7      "sistemPkk", $ibu->token );
8      $send = Cryptography::cryptoJsAesDecrypt (
8      "sistemPkk", $data['token'] );
9
10     if ( $db == $send ) {
11       return Response::json( ['status' => "SUCCESS" ]
11     );

```

```

12     }
13 }
14
15     return Response::json( ['status' => "FAILED"] );
16 }

```

**Kode Sumber 4.8. Implementasi Pemeriksaan Kesesuaian Token pada Server**

Kode Sumber 4.8 menunjukkan proses pemeriksaan token yang dilakukan pada *server* untuk mengolah data yang dikirimkan dari halaman konfirmasi token. Baris ke-7 dan ke-8 merupakan proses dekripsi token pada basis data dan token yang dikirimkan aplikasi. Proses perbandingan dilakukan pada baris ke-10 dan aplikasi dikirimkan balik respon atas proses pemeriksaan pada baris ke-11 (token cocok) dan ke-15 (token tidak cocok).

### 4.3. Implementasi Antarmuka Pengguna

Subbab ini akan menjelaskan implementasi antarmuka pengguna sesuai dengan rancangan antarmuka pengguna. Implementasi antarmuka pengguna akan dijelaskan pada subbab-subbab berikut.

#### 4.3.1. Halaman Login

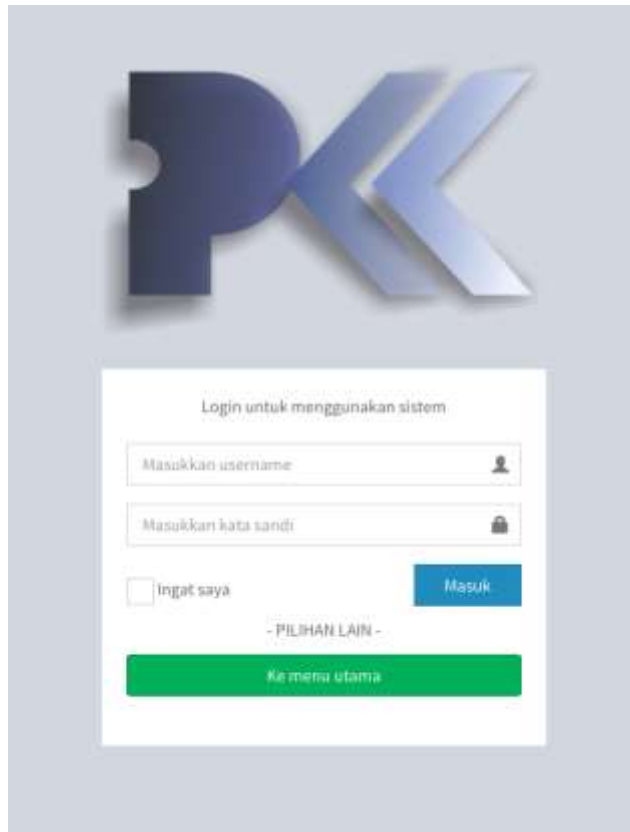
Antarmuka ini merupakan tampilan awal ketika pengguna memasuki sistem karena aplikasi web ini hanya dapat diakses oleh pengurus yang terdaftar. Pada halaman ini terdapat logo sistem dan kotak utama berisikan *form login* dan tombol-tombol navigasi. Di dalam *form login* terdapat dua buah kolom untuk memasukkan nama pengguna (*username*) dan kata sandi, sebuah *checkbox* untuk aktivasi fitur ingat saya, dan tombol masuk ke dalam sistem. Tombol-tombol navigasi yang disediakan adalah tombol lupa kata sandi, daftar akun pengguna baru, dan kembali ke menu utama. Tampilan dari halaman ini dapat dilihat pada Gambar 4.1.

#### 4.3.2. Halaman Verifikasi Akun Perangkat Bergerak

Antarmuka ini merupakan tampilan awal ketika pengguna melakukan *login* untuk pertama kalinya pada sebuah perangkat bergerak. Pada halaman ini terdapat judul halaman dan kotak teks untuk memasukkan token, serta sebuah tombol untuk mengirim



token agar divalidasi oleh sistem. Pada bagian bawah terdapat sebuah kotak informasi mendapatkan token. Tampilan dari halaman ini dapat dilihat pada Gambar 4.2.

The image shows a login interface on a light gray background. At the top center is a large, stylized logo consisting of a dark blue 'P' and two light blue 'K's. Below the logo is a white rectangular box containing the login form. The form has the title 'Login untuk menggunakan sistem' at the top. It includes two input fields: 'Masukkan username' with a user icon and 'Masukkan kata sandi' with a lock icon. Below these is a checkbox labeled 'Ingat saya' and a blue 'Masuk' button. At the bottom of the form is a green button labeled 'Ke menu utama'.

**Gambar 4.1. Implementasi Antarmuka Halaman Login**

#### **4.3.3. Halaman Profil Akun**

Antarmuka ini merupakan tampilan ketika pengguna menekan menu profil akun pada bagian *sidebar* setelah melakukan *login*. Pada halaman ini terdapat tiga buah kotak berisikan profil akun, nama pengguna, dan manajemen kata sandi. Di dalam profil akun

berisikan informasi-informasi seputar wilayah akun yang dimasukkan saat melakukan registrasi. Di dalam kotak nama pengguna terdapat kolom yang otomatis berisikan nama pengguna akun dan sebuah tombol simpan untuk mengubah nama pengguna. Di dalam kotak manajemen kata sandi terdapat tiga buah kolom untuk kata sandi lama, kata sandi baru, dan konfirmasi kata sandi, serta sebuah tombol simpan yang digunakan untuk menyimpan dan memvalidasi kata sandi baru yang akan digunakan. Tampilan dari halaman ini dapat dilihat pada Gambar 4.3.



**Gambar 4.2. Implementasi Antarmuka Halaman Verifikasi Akun Perangkat Bergerak**

[illegible]

### Gambar 4.3. Rancangan Antarmuka Halaman Profil Akun

*[Halaman ini sengaja dikosongkan]*

## **BAB V**

### **UJI COBA DAN EVALUASI**

Bab ini membahas pengujian dan evaluasi pada aplikasi yang dikembangkan. Pengujian yang dilakukan adalah pengujian fungsionalitas dan pengujian kerahasiaan data serta otentisitas pengguna yang diimplementasikan ke dalam sistem.

#### **5.1. Lingkungan Uji Coba**

Lingkungan uji coba yang digunakan dalam pembuatan Tugas Akhir ini meliputi perangkat lunak dan perangkat keras yang digunakan untuk melakukan uji coba implementasi sistem e-PKK *online*. Lingkungan uji coba terdiri dari 2 (dua) buah perangkat, yakni *laptop* untuk pengujian aplikasi web dan ponsel pintar (*smartphone*) untuk pengujian aplikasi perangkat bergerak dengan spesifikasi yang ditampilkan pada dan .

**Tabel 5.1. Lingkungan Uji Coba Aplikasi Web (*laptop*)**

Perangkat	Spesifikasi
Perangkat keras	Prosesor: 1.86 GHz Intel® Core™ 2 Duo Memori: 2.00 GB 1067 MHz DDR3
Perangkat lunak	Sistem Operasi: OS X El Capitan Versi 10.11.5 Bahasa Pemrograman: HTML5, PHP, SQL, JavaScript Kerangka Kerja: Laravel 5.1, PhoneGap Kakas Pembantu: StarUML, PowerDesigner, Sublime Text 3, MAMP

**Tabel 5.2. Lingkungan Uji Coba Aplikasi Perangkat Bergerak (*smartphone*)**

Merk	Samsung Galaxy S4
Prosesor	ARMv7 Processor rev 2 (v7I)
RAM	2.00 GB
Sistem Operasi	Android 5.0.1 Lollipop

#### **5.2. Skenario Uji Coba**

Pada subbab ini akan dijelaskan mengenai skenario uji coba yang telah dilakukan. Pengujian yang dilakukan adalah pengujian fungsionalitas, pengujian kerahasiaan data menggunakan ISO

25010, pengujian otentisitas pengguna menggunakan ISO 25010, dan pengujian kebergunaan. Pengujian fungsionalitas dilakukan menggunakan metode kotak hitam (*blackbox testing*), yaitu pengujian yang menekankan pada kesesuaian keluaran sistem. Pengujian menggunakan ISO 25010 dilakukan dengan menghitung nilai metrik yang dicantumkan pada Bab 2.3 dan Bab 2.4. Pengujian kebergunaan dilakukan dengan melakukan survei kepada pengguna.

### 5.2.1. Pengujian Fungsionalitas

Pengujian fungsionalitas sistem dilakukan dengan menyiapkan sejumlah skenario sebagai tolok ukur keberhasilan pengujian. Pengujian fungsionalitas pada Tugas Akhir ini dikhususkan untuk fitur pada kasus penggunaan pada Bab 3.3. Pengujian kebutuhan fungsionalitas dapat dijabarkan pada subbab-subbab berikut.

#### 5.2.1.1. Pengujian Fitur Melihat Profil Akun

Pengujian fitur ini merupakan pengujian terhadap kemampuan aplikasi dalam menampilkan profil akun pengguna. Rincian skenario pengujian untuk kasus penggunaan ini ditampilkan pada Tabel 5.3.

**Tabel 5.3. Pengujian Fitur Melihat Profil Akun**

Kode Pengujian	UT-001
Nama pengujian	Pengujian fitur melihat profil akun
Referensi Use Case	UC-155
Nama Use Case	Melihat profil akun
Tujuan Pengujian	Menguji fitur untuk menampilkan profil akun
Kondisi Awal	Sudah melakukan <i>login</i>
Langkah Pengujian	Menekan menu profil pada <i>sidebar</i>
Hasil yang diharapkan	Aplikasi menampilkan informasi mengenai wilayah akun dan otomatis mengisi kolom nama pengguna
Hasil yang didapatkan	Aplikasi menampilkan informasi mengenai wilayah akun dan otomatis mengisi kolom nama pengguna
Hasil pengujian	Berhasil
Kondisi Akhir	Pengguna disajikan halaman profil PKK seperti pada Gambar 5.1

Akun Saya Logout PPK

Profil PPK

Ubah PPK

Kode Wilayah

11.16.01.2012

Daerah

Jember

Provinsi

Jawa Timur

Kabupaten/Kota

Kab. Jember

Kecamatan

Jember

Desa/Kelurahan

Karangas

RW

01

RT

01

Username Pengguna

Username

alsh

Simpul username baru

Manajemen Kata Sandi Akun

Kata sandi lama:

Kata sandi baru:

Masukkan ulang kata sandi baru:

Simpul kata sandi baru

Menu Utama > Akun Saya

Gambar 5.1. Pengujian Fitur Melihat Profil Akun

Akun SayaPengguna PKK

Username terdapat di dalam

Profil PKK

Ubah PKK

Kode Wilayah

11.14.07.2012

Daerah

Bangka

Provinsi

Asah

Kabupaten/Kota

Kab. Bahr Jaya

Kecamatan

Indra Jaya

Desa/Kelurahan

Harauh Arah

RW

07

RT

01

Username Pengguna

Username

pkk@asah

Sesuaikan Email

Manajemen Kata Sandi Akun

Kata sandi lama:

Kata sandi baru:

Masukkan ulang kata sandi baru:

Sesuai kata sandi baru

Gambar 5.2. Pengujian Fitur Mengubah Nama Pengguna Skenario 1



### 5.2.1.2. Pengujian Fitur Mengubah Nama Pengguna

Pengujian fitur ini merupakan pengujian terhadap kemampuan aplikasi dalam mengolah nama pengguna. Rincian skenario pengujian untuk kasus penggunaan ini ditampilkan pada Tabel 5.4 dan Tabel 5.5.

**Tabel 5.4. Pengujian Fitur Mengubah Nama Pengguna Skenario 1**

Kode Pengujian	UT-002-1
Nama pengujian	Pengujian fitur mengubah nama pengguna
Referensi Use Case	UC-156
Nama Use Case	Ubah <i>username</i>
Tujuan Pengujian	Menguji fitur dalam mengubah nama pengguna akun
Kondisi Awal	Berada pada halaman profil akun
Langkah Pengujian	Mengubah konten pada kolom nama pengguna dengan nama pengguna yang valid lalu menekan tombol simpan
Hasil yang diharapkan	Aplikasi menampilkan kembali halaman profil akun dengan notifikasi keberhasilan perubahan nama pengguna dan kolom nama pengguna otomatis diisi dengan nama pengguna baru
Hasil yang didapatkan	Aplikasi menampilkan kembali halaman profil akun dengan notifikasi keberhasilan perubahan nama pengguna dan kolom nama pengguna otomatis diisi dengan nama pengguna baru
Hasil pengujian	Berhasil
Kondisi Akhir	Pengguna disajikan halaman profil PKK seperti pada Gambar 5.2

**Tabel 5.5. Pengujian Fitur Mengubah Nama Pengguna Skenario 2**

Kode Pengujian	UT-002-2
Nama pengujian	Pengujian fitur mengubah nama pengguna
Referensi Use Case	UC-156
Nama Use Case	Ubah <i>username</i>
Tujuan Pengujian	Menguji fitur dalam mengubah nama pengguna akun
Kondisi Awal	Berada pada halaman profil akun
Langkah Pengujian	Mengubah konten pada kolom nama pengguna dengan nama pengguna yang tidak valid, dalam hal ini dikosongkan, lalu menekan tombol simpan

Hasil yang diharapkan	Aplikasi menampilkan kembali halaman profil akun dengan notifikasi kegagalan perubahan nama pengguna beserta penyebabnya
Hasil yang didapatkan	Aplikasi menampilkan kembali halaman profil akun dengan notifikasi kegagalan perubahan nama pengguna beserta penyebabnya
Hasil pengujian	Berhasil
Kondisi Akhir	Terdapat peringatan pada kotak nama pengguna seperti pada Gambar 5.3

The image shows a web form for updating a user's profile. At the top, there is a header 'Username Pengguna' with a user icon. Below it, the label 'Username:' is followed by a text input field. The input field has a red border, indicating an error. Below the input field, a red error message reads 'Kolom username harus terisi'. At the bottom of the form, there is a blue button with the text 'Simpan username baru'.

**Gambar 5.3. Pengujian Fitur Mengubah Nama Pengguna Skenario 2**

### 5.2.1.3. Pengujian Fitur Mengubah Kata Sandi

Pengujian fitur ini merupakan pengujian terhadap kemampuan aplikasi dalam mengolah kata sandi akun. Rincian skenario pengujian untuk kasus penggunaan ini ditampilkan pada Tabel 5.6 dan Tabel 5.7.

**Tabel 5.6. Pengujian Fitur Mengubah Kata Sandi Skenario 1**

Kode Pengujian	UT-003-1
Nama pengujian	Pengujian fitur mengubah kata sandi
Referensi Use Case	UC-157
Nama Use Case	Ganti kata sandi
Tujuan Pengujian	Menguji fitur dalam mengubah kata sandi akun
Kondisi Awal	Berada pada halaman profil akun
Langkah Pengujian	Mengisi kolom kata sandi lama dengan kata sandi yang digunakan saat <i>login</i> dan mengisi kolom kata sandi baru beserta konfirmasinya dengan kata sandi baru berisikan 8 karakter lalu menekan tombol simpan

Hasil yang diharapkan	Aplikasi menampilkan kembali halaman profil akun dengan notifikasi keberhasilan perubahan kata sandi
Hasil yang didapatkan	Aplikasi menampilkan kembali halaman profil akun dengan notifikasi keberhasilan perubahan kata sandi
Hasil pengujian	Berhasil
Kondisi Akhir	Pengguna disajikan notifikasi keberhasilan pada halaman profil PKK seperti pada Gambar 5.4

**Tabel 5.7. Pengujian Fitur Mengubah Kata Sandi Skenario 2**

Kode Pengujian	UT-003-2
Nama pengujian	Pengujian fitur mengubah kata sandi
Referensi Use Case	UC-157
Nama Use Case	Ganti kata sandi
Tujuan Pengujian	Menguji fitur dalam mengubah kata sandi akun
Kondisi Awal	Berada pada halaman profil akun
Langkah Pengujian	Mengisi kolom kata sandi lama dengan kata sandi berbeda dengan yang digunakan saat <i>login</i> dan mengisi kolom kata sandi baru beserta konfirmasinya dengan kata sandi baru berisikan 8 karakter lalu menekan tombol simpan
Hasil yang diharapkan	Aplikasi menampilkan kembali halaman profil akun dengan notifikasi kegagalan perubahan kata sandi
Hasil yang didapatkan	Aplikasi menampilkan kembali halaman profil akun dengan notifikasi kegagalan perubahan kata sandi
Hasil pengujian	Berhasil
Kondisi Akhir	Pengguna disajikan notifikasi kegagalan pada halaman profil PKK seperti pada Gambar 5.5

**Kata sandi berhasil diperbarui**

**Gambar 5.4. Pengujian Fitur Mengubah Kata Sandi Skenario 1**

**Gagal merubah kata sandi: Kata sandi tidak cocok**

**Gambar 5.5. Pengujian Fitur Mengubah Kata Sandi Skenario 2**

#### 5.2.1.4. Pengujian Fitur *Reset Token Akun*

Pengujian fitur ini merupakan pengujian terhadap kemampuan aplikasi dalam mendapatkan ulang token akun. Rincian skenario pengujian untuk kasus penggunaan ini ditampilkan pada Tabel 5.8.

**Tabel 5.8. Pengujian Fitur *Reset Token Akun***

Kode Pengujian	UT-004
Nama pengujian	Pengujian fitur <i>reset</i> token akun
Referensi Use Case	UC-162
Nama Use Case	<i>Reset</i> token akun PKK
Tujuan Pengujian	Menguji fitur dalam mendapatkan ulang token baru akun pengguna perangkat bergerak
Kondisi Awal	Berada pada halaman anggota PKK
Langkah Pengujian	Menekan tombol <i>reset</i> token pada suatu baris anggota PKK
Hasil yang diharapkan	Aplikasi menyimpan token baru untuk pengguna tersebut, pengguna perangkat bergerak harus melakukan konfirmasi token akun saat <i>login</i> , dan muncul notifikasi pada halaman anggota PKK
Hasil yang didapatkan	Aplikasi menyimpan token baru untuk pengguna tersebut, pengguna perangkat bergerak harus melakukan konfirmasi token akun saat <i>login</i> , dan muncul notifikasi pada halaman anggota PKK
Hasil pengujian	Berhasil
Kondisi Akhir	Pengguna disajikan notifikasi keberhasilan <i>reset</i> token akun seperti pada Gambar 5.6



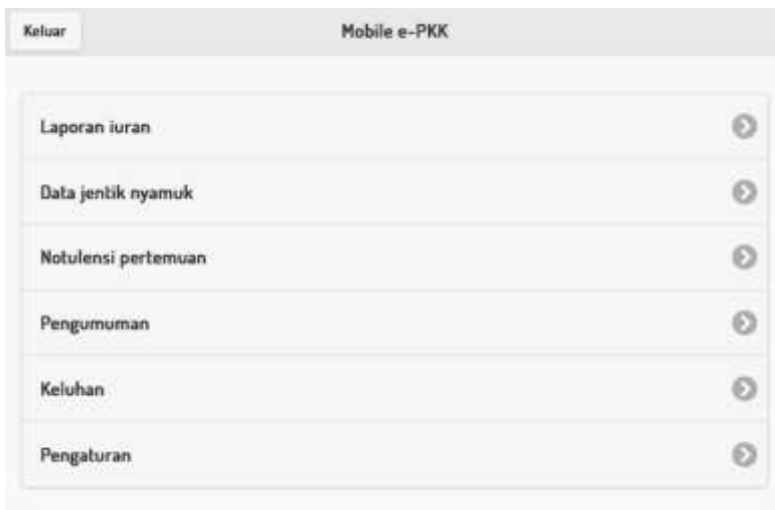
**Gambar 5.6. Pengujian Fitur *Reset Token Akun***

### 5.2.1.5. Pengujian Fitur Verifikasi Akun

Pengujian fitur ini merupakan pengujian terhadap kemampuan aplikasi dalam mengenali token akun. Rincian skenario pengujian untuk kasus penggunaan ini ditampilkan pada Tabel 5.9.

**Tabel 5.9. Pengujian Fitur Verifikasi Akun**

Kode Pengujian	UT-005
Nama pengujian	Pengujian fitur verifikasi akun
Referensi Use Case	UC-201
Nama Use Case	Verifikasi akun PKK
Tujuan Pengujian	Menguji fitur dalam mengenali token akun pengguna perangkat bergerak
Kondisi Awal	Berada pada halaman konfirmasi token akun
Langkah Pengujian	Memasukkan token yang sesuai
Hasil yang diharapkan	Aplikasi mengenali token akun pengguna dan pengguna masuk ke dalam sistem
Hasil yang didapatkan	Aplikasi mengenali token akun pengguna dan pengguna masuk ke dalam sistem
Hasil pengujian	Berhasil
Kondisi Akhir	Pengguna disajikan menu utama aplikasi seperti pada Gambar 5.7



**Gambar 5.7. Pengujian Fitur Verifikasi Akun**

### 5.2.1.6. Pengujian Fitur Mengelola Akun Pengguna

Pengujian fitur ini merupakan pengujian terhadap kemampuan mengelola akun pengguna. Rincian skenario pengujian untuk kasus penggunaan ini ditampilkan pada Tabel 5.9.

**Tabel 5.10. Pengujian Fitur Mengelola Akun Pengguna**

Kode Pengujian	UT-006
Nama pengujian	Pengujian fitur mengelola akun pengguna
Referensi Use Case	UC-601
Nama Use Case	Mengelola akun pengguna
Tujuan Pengujian	Menguji fitur dalam menampilkan akun pengguna
Kondisi Awal	Sudah melakukan <i>login</i> sebagai administrator
Langkah Pengujian	Memilih menu manajemen akun pengguna pada <i>sidebar</i>
Hasil yang diharapkan	Aplikasi menampilkan halaman akun pengguna berisikan daftar akun pengguna dan kotak pemilihan lokasi
Hasil yang didapatkan	Aplikasi menampilkan halaman akun pengguna berisikan daftar akun pengguna dan kotak pemilihan lokasi
Hasil pengujian	Berhasil
Kondisi Akhir	Pengguna disajikan halaman akun pengguna seperti pada Gambar 5.8



**Gambar 5.8. Pengujian Fitur Mengelola Akun Pengguna**

### 5.2.2. Pengujian Kerahasiaan Data dan Otentisitas Pengguna Menggunakan ISO 25010

Pengujian kerahasiaan data dan otentisitas pengguna dilakukan dengan menghitung nilai metrik yang dicantumkan di dalam standar ISO 25010 dan dijelaskan pada Bab 3.2. Deskripsi aturan penulisan tabel pengujian dijelaskan pada Tabel 5.11.

**Tabel 5.11. Deskripsi Aturan Penulisan Tabel Pengujian**

<b>Metrik</b>	<b>Kolom</b>	<b>Deskripsi</b>
Kemampuan Pengendalian Akses	Fitur	Subjek fitur pada aplikasi
	Jalur/ <i>route</i>	Halaman tujuan jalur/ <i>route</i>
	Jumlah	Jumlah jalur yang perlu diberi otorisasi khusus
	Akses	Keterangan apakah jalur belum diberi otorisasi khusus
Ketepatan Enkripsi Data	Aplikasi	Aplikasi di dalam sistem
	Data	Data yang perlu dienkrpsi/didekripsi
	Jumlah	Jumlah data yang perlu dienkrpsi / dekripsi
	Hasil Enkripsi	Keterangan apakah hasil enkripsi tepat
Kekuatan Kriptografi Algoritma	Aplikasi	Aplikasi di dalam sistem
	Algoritma Kriptografi	Algoritma kriptografi yang tersedia
	Jumlah	Jumlah algoritma kriptografi yang tersedia
	Proses Tidak Sukses	Keterangan apakah proses kriptografi mengeluarkan hasil tidak tepat
Kesesuaian Protokol Otentikasi	Aplikasi	Aplikasi di dalam sistem
	Protokol Otentikasi	Protokol otentikasi yang diperlukan sistem
	Jumlah	Jumlah protokol otentikasi yang diperlukan
	Status	Keterangan apakah protokol otentikasi disediakan sistem

Metrik	Kolom	Deskripsi
Kesesuaian Aturan Otentikasi	<i>Platform</i>	<i>Platform</i> aplikasi di dalam sistem
	Aturan Otentikasi	Aturan otentikasi yang diperlukan sebuah sistem yang aman (sesuai kebutuhan)
	Sistem PKK	Keterangan implementasi aturan otentikasi pada sistem PKK
	Sistem Posyandu	Keterangan implementasi aturan otentikasi pada sistem Posyandu
	Total	Total aturan otentikasi yang sudah diimplementasikan

Pengujian akan dilakukan dalam dua tahap dan sesuai dengan perhitungan yang dijelaskan pada Bab 3.2. Pengujian kualitas ini dapat dijabarkan pada subbab-subbab berikut.

#### 5.2.2.1. Pengujian Tahap Pertama

Pengujian tahap pertama dilakukan pada sistem e-PKK *online* yang sudah ada. Penjabaran metrik-metrik pengujian dapat dilihat pada Tabel 5.12, Tabel 5.13, Tabel 5.14, Tabel 5.15, dan Tabel 5.16. Penjelasan hasil nilai untuk tiap metrik akan dituliskan setelah tiap tabel pengujian.

**Tabel 5.12. Pengujian Tahap Pertama (Kemampuan Pengendalian Akses)**

Fitur	Jalur / Route	Jumlah	Akses
<b>Aplikasi Web PKK</b>			
Data PKK	Halaman utama data PKK	5	Belum
	Tambah data PKK		Belum
	Ubah data PKK		Belum
	Hapus data PKK		Belum
	Lihat rincian data PKK		Belum
Periode Kepengurusan	Halaman utama periode kepengurusan	4	Belum
	Tambah periode		Belum
	Ubah periode		Belum
	Hapus periode		Belum



Fitur	Jalur / Route	Jumlah	Akses
Jabatan Pengurus	Halaman utama jabatan pengurus	4	Belum
	Tambah jabatan		Belum
	Ubah jabatan		Belum
	Hapus jabatan		Belum
Pengurus PKK	Halaman utama pengurus PKK	4	Belum
	Tambah pengurus		Belum
	Ubah pengurus		Belum
	Hapus pengurus		Belum
Anggota PKK	Halaman utama anggota PKK	5	Belum
	Tambah anggota		Belum
	Ubah anggota		Belum
	Hapus anggota		Belum
	Lihat rincian anggota		Belum
Kas PKK	Halaman utama kas PKK	7	Belum
	Tambah kas pengeluaran		Belum
	Tambah kas pemasukan		Belum
	Ubah kas pengeluaran		Belum
	Ubah kas pemasukan		Belum
	Hapus kas pengeluaran		Belum
	Hapus kas pemasukan		Belum
Jenis Kas PKK	Halaman utama jenis kas PKK	7	Belum
	Tambah jenis kas pengeluaran		Belum
	Tambah jenis kas pemasukan		Belum
	Ubah jenis kas pengeluaran		Belum
	Ubah jenis kas pemasukan		Belum
	Hapus jenis kas pengeluaran		Belum
	Hapus jenis kas pemasukan		Belum
Kegiatan PKK	Halaman utama kegiatan PKK	4	Belum
	Tambah kegiatan		Belum

<b>Fitur</b>	<b>Jalur / Route</b>	<b>Jumlah</b>	<b>Akses</b>
	Ubah kegiatan		Belum
	Hapus kegiatan		Belum
Absen	Halaman utama absen	4	Belum
	Tambah absen		Belum
	Hapus absen		Belum
Notulensi	Halaman utama notulensi	4	Belum
	Tambah notulensi		Belum
	Ubah notulensi		Belum
	Hapus notulensi		Belum
Pengumuman	Halaman utama pengumuman	5	Belum
	Tambah pengumuman		Belum
	Ubah pengumuman		Belum
	Hapus pengumuman		Belum
	Lihat rincian pengumuman		Belum
Laporan Bidang	Halaman utama laporan bidang	5	Belum
	Pilih tahun data jentik nyamuk		Belum
	Tambah laporan bidang		Belum
	Hapus laporan bidang		Belum
	Unduh laporan bidang		Belum
Data Jentik Nyamuk	Halaman utama data jentik nyamuk	4	Belum
	Tambah data jentik nyamuk		Belum
	Ubah data jentik nyamuk		Belum
	Hapus data jentik nyamuk		Belum
Keluhan	Halaman utama keluhan	4	Belum
	Hapus keluhan		Belum
	Lihat rincian keluhan		Belum
	Tambah komentar		Belum
<b>Total</b>		66	66
<b>Aplikasi Perangkat Bergerak PKK</b>			

Fitur	Jalur / Route	Jumlah	Akses
Iuran	Halaman laporan iuran	1	Ada
Jentik	Halaman jentik nyamuk	1	Ada
Notulensi	Halaman notulensi pertemuan	1	Ada
Pengumuman	Halaman pengumuman	1	Ada
Keluhan	Halaman tambah keluhan	3	Ada
	Halaman daftar keluhan		Ada
	Halaman kirim komentar		Ada
<b>Total</b>		<b>7</b>	<b>0</b>
<b>Aplikasi Web Posyandu</b>			
Balita	Halaman utama balita	4	Belum
	Tambah balita		Belum
	Ubah balita		Belum
	Hapus balita		Belum
Ibu Balita	Halaman utama ibu balita	4	Belum
	Tambah ibu balita		Belum
	Ubah ibu balita		Belum
	Hapus ibu balita		Belum
Penimbangan	Halaman utama penimbangan	4	Belum
	Tambah penimbangan		Belum
	Ubah penimbangan		Belum
	Hapus penimbangan		Belum
Pemberian Imunisasi	Halaman utama pemberian imunisasi	4	Belum
	Tambah pemberian imunisasi		Belum
	Ubah pemberian imunisasi		Belum
	Hapus pemberian imunisasi		Belum
Pemberian Kapsul	Halaman utama pemberian kapsul	4	Belum
	Tambah pemberian kapsul		Belum
	Ubah pemberian kapsul		Belum
	Hapus pemberian kapsul		Belum

Fitur	Jalur / Route	Jumlah	Akses
Pengurus Posyandu	Halaman utama pengurus Posyandu	4	Belum
	Tambah pengurus Posyandu		Belum
	Ubah pengurus Posyandu		Belum
	Hapus pengurus Posyandu		Belum
Kas Posyandu	Halaman utama kas Posyandu	4	Belum
	Tambah kas Posyandu		Belum
	Ubah kas Posyandu		Belum
	Hapus kas Posyandu		Belum
Absen Balita	Halaman utama absen balita	4	Belum
	Tambah absen balita		Belum
	Ubah absen balita		Belum
	Hapus absen balita		Belum
Keluhan	Halaman utama keluhan	5	Belum
	Hapus keluhan		Belum
	Lihat rincian keluhan		Belum
	Tambah jawaban keluhan		Belum
	Hapus jawaban keluhan		Belum
<b>Total</b>		46	46
<b>Aplikasi Perangkat Bergerak Posyandu</b>			
Nutrisi	Rekomendasi nutrisi	3	Ada
	Bolehkah?		Ada
	Informasi alergi dan gizi		Ada
Perkembangan	Informasi perkembangan balita	1	Ada
P3K	Informasi P3K	1	Ada
KMS	Memilih anak	11	Ada
	Lihat data anak		Ada
	Tambah data anak		Ada
	Ubah data anak		Ada
	Lihat grafik KMS		Ada

Fitur	Jalur / Route	Jumlah	Akses
	Mengisi KMS		Ada
	Lihat rincian data KMS		Ada
	Halaman imunisasi		Ada
	Tambah imunisasi		Ada
	Halaman vitamin		Ada
	Tambah vitamin		Ada
History	Memilih anak	5	Ada
	Lihat grafik KMS		Ada
	Lihat rincian data KMS		Ada
	Lihat imunisasi		Ada
	Lihat vitamin		Ada
Keluhan	Kirim keluhan	2	Ada
	Lihat keluhan		Ada
<b>Total</b>		23	0

Hasil pengujian metrik kemampuan pengendalian akses dijelaskan pada poin-poin berikut:

- Jumlah jalur yang belum diberi otorisasi ( $A_{KPA}$ ) = 112
- Jumlah jalur yang perlu otorisasi ( $B_{KPA}$ ) = 142
- Hasil perhitungan =  $\left(1 - \frac{112}{142}\right) = (1 - 0,79) = 0,21$

**Tabel 5.13. Pengujian Tahap Pertama (Ketepatan Enkripsi Data)**

Aplikasi	Data	Jumlah	Hasil Enkripsi
Web PKK	Kata sandi saat <i>login</i>	2	Tepat
	Kata sandi saat pendaftaran pengguna perangkat bergerak baru		Tidak
Perangkat Bergerak PKK	Kata sandi saat <i>login</i>	4	Tidak
	Ganti kata sandi (kata sandi lama)		Tidak
	Ganti kata sandi (kata sandi baru)		Tidak
	Ganti kata sandi (konfirmasi)		Tidak

Aplikasi	Data	Jumlah	Hasil Enkripsi
Web Posyandu	Kata sandi saat <i>login</i>	2	Tepat
	Kata sandi saat pendaftaran pengguna perangkat bergerak baru		Tidak
Perangkat Bergerak Posyandu	Kata sandi saat <i>login</i>	1	Tidak
Total		9	2

Hasil pengujian metrik ketepatan enkripsi data dijelaskan pada poin-poin berikut:

- Jumlah data yang tepat dienkripsi/didekripsi ( $A_{KED}$ ) = 2
- Jumlah data yang perlu dienkripsi/didekripsi ( $B_{KED}$ ) = 9
- Hasil perhitungan =  $\frac{2}{9} = 0,22$

**Tabel 5.14. Pengujian Tahap Pertama (Kekuatan Kriptografi Algoritma)**

Aplikasi	Algoritma Kriptografi	Jumlah	Proses Tidak Sukses
Web PKK	Cartalyst Sentinel Hash: fungsi <code>bcrypt()</code> → DES	1	Sukses
Web Posyandu	Cartalyst Sentinel Hash: fungsi <code>bcrypt()</code> → DES	1	Sukses
Total		2	2

Hasil pengujian metrik kekuatan kriptografi algoritma dijelaskan pada poin-poin berikut:

- Jumlah fungsi dengan keluaran tidak tepat ( $A_{KKA}$ ) = 0
- Jumlah fungsi kriptografi yang digunakan ( $B_{KKA}$ ) = 2
- Hasil perhitungan =  $\left(1 - \frac{0}{2}\right) = (1 - 0) = 1$

**Tabel 5.15. Pengujian Tahap Pertama (Kesesuaian Protokol Otentikasi)**

Aplikasi	Protokol Otentikasi	Jumlah	Status
Web PKK	Nama pengguna	3	Ada

Aplikasi	Protokol Otentikasi	Jumlah	Status
	Kata sandi		Ada
	ID pengguna		Tidak
Perangkat Bergerak PKK	Nomor telepon	2	Ada
	Kata sandi		Ada
Web Posyandu	Nama pengguna	3	Ada
	Kata sandi		Ada
	ID pengguna		Tidak
Perangkat Bergerak Posyandu	Nomor telepon	2	Ada
	Kata sandi		Ada
<b>Total</b>		10	8

Hasil pengujian metrik kesesuaian protokol otentikasi dijelaskan pada poin-poin berikut:

- Jumlah protokol yang digunakan ( $A_{KPO}$ ) = 8
- Jumlah protokol yang dibutuhkan ( $B_{KPO}$ ) = 10
- Hasil perhitungan =  $\frac{8}{10} = 0,8$

**Tabel 5.16. Pengujian Tahap Pertama (Kesesuaian Aturan Otentikasi)**

Platform	Aturan Otentikasi	Sistem PKK	Sistem Posyandu	Total
Web	Login	V	V	2
	Registrasi	X	X	0
	Ubah Kata Sandi	X	X	0
	Perangkat Tengah	X	X	0
Perangkat Bergerak	Login	V	V	2
	Registrasi	X	X	0
	Ubah Kata Sandi	V	X	1
	Verifikasi Akun	X	X	0
<b>Total</b>				5

Hasil pengujian metrik kesesuaian aturan otentikasi dijelaskan pada poin-poin berikut:

- Jumlah aturan yang diimplementasikan ( $A_{KAO}$ ) = 5
- Jumlah aturan yang dibutuhkan ( $B_{KAO}$ ) = 16
- Hasil perhitungan =  $\frac{5}{16} = 0,3125$

### 5.2.2.2. Pengujian Tahap Kedua

Pengujian tahap kedua dilakukan pada sistem yang sudah diberi tambahan fitur mengenai metrik yang diujikan, yang dijelaskan pada Bab 3.5, sudah diimplementasikan. Penjabaran metrik-metrik pengujian dapat dilihat pada Tabel 5.17, Tabel 5.18, Tabel 5.19, Tabel 5.20, dan Tabel 5.21. Penjelasan hasil nilai untuk tiap metrik akan dituliskan setelah tiap tabel pengujian.

**Tabel 5.17. Pengujian Tahap Kedua (Kemampuan Pengendalian Akses)**

Fitur	Jalur / Route	Jumlah	Akses
<b>Aplikasi Web PKK</b>			
Profil Akun	Halaman profil akun	3	Ada
	Ubah nama pengguna		Ada
	Ubah kata sandi		Ada
Periode Kepengurusan	Halaman utama periode kepengurusan	4	Ada
	Tambah periode		Ada
	Ubah periode		Ada
	Hapus periode		Ada
Jabatan Pengurus	Halaman utama jabatan pengurus	4	Ada
	Tambah jabatan		Ada
	Ubah jabatan		Ada
	Hapus jabatan		Ada
Pengurus PKK	Halaman utama pengurus PKK	4	Ada
	Tambah pengurus		Ada
	Ubah pengurus		Ada
	Hapus pengurus		Ada



Fitur	Jalur / Route	Jumlah	Akses
Anggota PKK	Halaman utama anggota PKK	6	Ada
	Tambah anggota		Ada
	Ubah anggota		Ada
	Hapus anggota		Ada
	Lihat rincian anggota		Ada
	Reset token akun perangkat bergerak		Ada
Kas PKK	Halaman utama kas PKK	7	Ada
	Tambah kas pengeluaran		Ada
	Tambah kas pemasukan		Ada
	Ubah kas pengeluaran		Ada
	Ubah kas pemasukan		Ada
	Hapus kas pengeluaran		Ada
	Hapus kas pemasukan		Ada
Jenis Kas PKK	Halaman utama jenis kas PKK	7	Ada
	Tambah jenis kas pengeluaran		Ada
	Tambah jenis kas pemasukan		Ada
	Ubah jenis kas pengeluaran		Ada
	Ubah jenis kas pemasukan		Ada
	Hapus jenis kas pengeluaran		Ada
	Hapus jenis kas pemasukan		Ada
Kegiatan PKK	Halaman utama kegiatan PKK	4	Ada
	Tambah kegiatan		Ada
	Ubah kegiatan		Ada
	Hapus kegiatan		Ada
Absen	Halaman utama absen	3	Ada
	Tambah absen		Ada
	Hapus absen		Ada
Notulensi	Halaman utama notulensi	4	Ada
	Tambah notulensi		Ada

Fitur	Jalur / Route	Jumlah	Akses
	Ubah notulensi		Ada
	Hapus notulensi		Ada
Pengumuman	Halaman utama pengumuman	5	Ada
	Tambah pengumuman		Ada
	Ubah pengumuman		Ada
	Hapus pengumuman		Ada
	Lihat rincian pengumuman		Ada
Laporan Bidang	Halaman utama laporan bidang	4	Ada
	Tambah laporan bidang		Ada
	Hapus laporan bidang		Ada
	Unduh laporan bidang		Ada
Data Jentik Nyamuk	Halaman utama data jentik nyamuk	5	Ada
	Pilih tahun data jentik nyamuk		Ada
	Tambah data jentik nyamuk		Ada
	Ubah data jentik nyamuk		Ada
	Hapus data jentik nyamuk		Ada
Keluhan	Halaman utama keluhan	4	Ada
	Hapus keluhan		Ada
	Lihat rincian keluhan		Ada
	Tambah komentar		Ada
<b>Total</b>		60	0
<b>Aplikasi Perangkat Bergerak PKK</b>			
Sama dengan pengujian pertama			
<b>Total</b>		7	0
<b>Aplikasi Web Posyandu</b>			
Profil Akun	Halaman profil akun	3	Ada
	Ubah nama pengguna		Ada
	Ubah kata sandi		Ada
Balita	Halaman utama balita	4	Ada

Fitur	Jalur / Route	Jumlah	Akses
	Tambah balita		Ada
	Ubah balita		Ada
	Hapus balita		Ada
Ibu Balita	Halaman utama ibu balita	5	Ada
	Tambah ibu balita		Ada
	Ubah ibu balita		Ada
	Hapus ibu balita		Ada
	Reset token akun perangkat bergerak		Ada
Penimbangan	Halaman utama penimbangan	4	Ada
	Tambah penimbangan		Ada
	Ubah penimbangan		Ada
	Hapus penimbangan		Ada
Pemberian Imunisasi	Halaman utama pemberian imunisasi	4	Ada
	Tambah pemberian imunisasi		Ada
	Ubah pemberian imunisasi		Ada
	Hapus pemberian imunisasi		Ada
Pemberian Kapsul	Halaman utama pemberian kapsul	4	Ada
	Tambah pemberian kapsul		Ada
	Ubah pemberian kapsul		Ada
	Hapus pemberian kapsul		Ada
Pengurus Posyandu	Halaman utama pengurus Posyandu	4	Ada
	Tambah pengurus Posyandu		Ada
	Ubah pengurus Posyandu		Ada
	Hapus pengurus Posyandu		Ada
Kas Posyandu	Halaman utama kas Posyandu	4	Ada
	Tambah kas Posyandu		Ada
	Ubah kas Posyandu		Ada
	Hapus kas Posyandu		Ada
Absen Balita	Halaman utama absen balita	4	Ada

Fitur	Jalur / Route	Jumlah	Akses
	Tambah absen balita		Ada
	Ubah absen balita		Ada
	Hapus absen balita		Ada
Keluhan	Halaman utama keluhan	5	Ada
	Hapus keluhan		Ada
	Lihat rincian keluhan		Ada
	Tambah jawaban keluhan		Ada
	Hapus jawaban keluhan		Ada
<b>Total</b>		50	0
<b>Aplikasi Perangkat Bergerak Posyandu</b>			
Sama dengan pengujian pertama			
<b>Total</b>		23	0
<b>Administrator</b>			
PKK	Halaman utama kelola akun	4	Ada
	Tambah akun		Ada
	Hapus akun		Ada
	Reset kata sandi		Ada
Posyandu	Halaman utama kelola akun	4	Ada
	Tambah akun		Ada
	Hapus akun		Ada
	Reset kata sandi		Ada
<b>Total</b>		8	0

Hasil pengujian metrik kemampuan pengendalian akses dijelaskan pada poin-poin berikut:

- Jumlah jalur yang belum diberi otorisasi ( $A_{KPA}$ ) = 0
- Jumlah jalur yang perlu otorisasi ( $B_{KPA}$ ) = 148
- Hasil perhitungan =  $\left(1 - \frac{0}{148}\right) = (1 - 0) = 1$

**Tabel 5.18. Pengujian Tahap Kedua (Ketepatan Enkripsi Data)**

Aplikasi	Data	Jumlah	Hasil Enkripsi
Web PKK	Kata sandi saat <i>login</i>	11	Tepat
	Kata sandi perangkat bergerak saat pendaftaran pengguna perangkat bergerak		Tepat
	Kata sandi perangkat bergerak saat mengubah kata sandi akun perangkat bergerak anggota PKK		Tepat
	Kata sandi akun web saat mendaftarkan akun baru (administrator)		Tepat
	Kata sandi akun web saat <i>reset</i> kata sandi akun (administrator)		Tepat
	Token pengguna saat mendaftarkan akun pengguna perangkat bergerak		Tepat
	Token pengguna saat mengubah kata sandi akun anggota PKK		Tepat
	Token pengguna saat <i>reset</i> token		Tepat
	Ganti kata sandi (kata sandi lama)		Tepat
	Ganti kata sandi (kata sandi baru)		Tepat
	Ganti kata sandi (konfirmasi)		Tepat
Perangkat Bergerak PKK	Kata sandi saat <i>login</i>	5	Tepat
	Ganti kata sandi (kata sandi lama)		Tepat
	Ganti kata sandi (kata sandi baru)		Tepat
	Ganti kata sandi (konfirmasi)		Tepat
	Token saat konfirmasi akun		Tepat
Web Posyandu	Kata sandi saat <i>login</i>	11	Tepat
	Kata sandi perangkat bergerak saat pendaftaran pengguna perangkat bergerak		Tepat

Aplikasi	Data	Jumlah	Hasil Enkripsi
	Kata sandi perangkat bergerak saat mengubah kata sandi akun perangkat bergerak ibu balita		Tepat
	Kata sandi akun web saat mendaftarkan akun baru (administrator)		Tepat
	Kata sandi akun web saat <i>reset</i> kata sandi akun (administrator)		Tepat
	Token pengguna saat mendaftarkan akun pengguna perangkat bergerak		Tepat
	Token pengguna saat mengubah kata sandi akun ibu balita		Tepat
	Token pengguna saat <i>reset</i> token		Tepat
	Ganti kata sandi (kata sandi lama)		Tepat
	Ganti kata sandi (kata sandi baru)		Tepat
	Ganti kata sandi (konfirmasi)		Tepat
Perangkat Bergerak Posyandu	Kata sandi saat <i>login</i>	2	Tepat
	Token saat konfirmasi akun		Tepat
<b>Total</b>		29	29

Hasil pengujian metrik ketepatan enkripsi data dijelaskan pada poin-poin berikut:

- Jumlah data yang tepat dienkripsi/didekripsi ( $A_{\text{KED}}$ ) = 29
- Jumlah data yang perlu dienkripsi/didekripsi ( $B_{\text{KED}}$ ) = 29
- Hasil perhitungan =  $\frac{29}{29} = 1$

**Tabel 5.19. Pengujian Tahap Kedua (Kekuatan Kriptografi Algoritma)**

Aplikasi	Algoritma Kriptografi	Jumlah	Proses Tidak Sukses
Web PKK	Laravel Auth Hash: bcrypt → MD5	2	Sukses
	CryptoJS: AES		Sukses

Aplikasi	Algoritma Kriptografi	Jumlah	Proses Tidak Sukses
Perangkat Bergerak PKK	CryptoJS: AES	1	Sukses
Web Posyandu	Cartalyst Sentinel Hash: fungsi bcrypt() → DES	2	Sukses
	CryptoJS: AES		Sukses
Perangkat Bergerak Posyandu	CryptoJS: AES	1	Sukses
<b>Total</b>		6	0

Hasil pengujian metrik kekuatan kriptografi algoritma dijelaskan pada poin-poin berikut:

- Jumlah fungsi dengan keluaran tidak tepat ( $A_{KKA}$ ) = 0
- Jumlah fungsi kriptografi yang digunakan ( $B_{KKA}$ ) = 6
- Hasil perhitungan =  $\left(1 - \frac{0}{6}\right) = (1 - 0) = 1$

**Tabel 5.20. Pengujian Tahap Kedua (Kesesuaian Protokol Otentikasi)**

Aplikasi	Identitas Subjek yang Dibutuhkan	Jumlah (B)	Ada (A)
Web PKK	Nama pengguna	3	Ada
	Kata sandi		Ada
	ID pengguna		Ada
Perangkat Bergerak PKK	Nomor telepon	3	Ada
	Kata sandi		Ada
	Token akun		Ada
Web Posyandu	Nama pengguna	3	Ada
	Kata sandi		Ada
	ID pengguna		Ada
Perangkat Bergerak Posyandu	Nomor telepon	3	Ada
	Kata sandi		Ada

Aplikasi	Identitas Subjek yang Dibutuhkan	Jumlah (B)	Ada (A)
	Token akun		Ada
<b>Total</b>		12	12

Hasil pengujian metrik kesesuaian protokol otentikasi dijelaskan pada poin-poin berikut:

- Jumlah protokol yang digunakan ( $A_{KPO}$ ) = 12
- Jumlah protokol yang dibutuhkan ( $B_{KPO}$ ) = 12
- Hasil perhitungan =  $\frac{12}{12} = 1$

**Tabel 5.21. Pengujian Tahap Kedua (Kesesuaian Aturan Otentikasi)**

Platform	Aturan Otentikasi (B)	Sistem PKK	Sistem Posyandu	Total (A)
Web	Login	V	V	2
	Registrasi	V	V	2
	Ubah Kata Sandi	V	V	2
	Perangkat Tengah	V	V	2
Perangkat Bergerak	Login	V	V	2
	Registrasi	V	V	2
	Ubah Kata Sandi	V	V	2
	Verifikasi Akun	V	V	2
<b>Total</b>				16

Hasil pengujian metrik kesesuaian aturan otentikasi dijelaskan pada poin-poin berikut:

- Jumlah aturan yang diimplementasikan ( $A_{KAO}$ ) = 16
- Jumlah aturan yang dibutuhkan ( $B_{KAO}$ ) = 16
- Hasil perhitungan =  $\frac{16}{16} = 1$



### 5.3. Evaluasi

#### 5.3.1. Evaluasi Pengujian Fungsionalitas

Rangkuman mengenai hasil pengujian fungsionalitas dapat dilihat pada Tabel 5.22. Berdasarkan data pada tabel tersebut, semua skenario pengujian berhasil dan berjalan dengan lancar. Oleh karena itu, dapat ditarik kesimpulan bahwa fungsionalitas sistem tetap berjalan sebagaimana fungsi seharusnya.

**Tabel 5.22. Rangkuman Hasil Pengujian Fungsionalitas**

Kode	Nama	Skenario	Hasil
UT-001	Pengujian fitur melihat profil akun		Berhasil
UT-002-1	Pengujian fitur mengubah nama pengguna	Skenario 1	Berhasil
UT-002-2		Skenario 2	Berhasil
UT-003-1	Pengujian fitur mengubah kata sandi	Skenario 1	Berhasil
UT-003-2		Skenario 2	Berhasil
UT-004	Pengujian fitur <i>reset</i> token akun		Berhasil
UT-005	Pengujian fitur verifikasi akun		Berhasil
UT-006	Pengujian fitur mengelola akun pengguna		Berhasil

#### 5.3.2. Evaluasi Pengujian Kerahasiaan Data dan Otentisitas Pengguna Menggunakan ISO 25010

Rangkuman mengenai hasil pengujian kerahasiaan data dan otentisitas pengguna menggunakan ISO 25010 dapat dilihat pada Tabel 5.23. Nilai tiap tahap didapatkan dari perhitungan metrik yang dilakukan pada bab 5.2.2.

**Tabel 5.23. Rangkuman Hasil Pengujian ISO 25010**

Metrik	Tahap 1	Tahap 2
Kemampuan Pengendalian Akses	0,21	1
Ketepatan Enkripsi Data	0,22	1
Kekuatan Kriptografi Algoritma	1	1
Kesesuaian Protokol Otentikasi	0,8	1
Kesesuaian Aturan Otentikasi	0,3125	1

Penjabaran hasil pengujian kerahasiaan data dan otentisitas pengguna pada tabel di atas menunjukkan bahwa sistem e-PKK *online* yang sudah dimodifikasi sudah memenuhi standar kualitas pada metrik yang diujikan, dikarenakan sudah mendapatkan nilai maksimal (1) pada tiap metriknya. Pengujian tahap pertama pada metrik kemampuan pengendalian akses mendapatkan nilai 0,21 dikarenakan banyaknya jalur yang tidak diberi otorisasi khusus. Metrik ketepatan enkripsi data pada pengujian tahap pertama mendapatkan nilai 0,22 dikarenakan banyaknya data penting pengguna yang tidak dilakukan enkripsi pada proses pertukaran data antar aplikasi. Metrik kekuatan kriptografi algoritma pada pengujian tahap pertama sudah mendapatkan nilai maksimal dikarenakan fungsi *Hash* milik *Sentinel 2.0* sudah mengeluarkan hasil yang tepat. Metrik kesesuaian protokol otentikasi mendapatkan nilai 0,8 pada pengujian tahap pertama, hal ini dikarenakan salah satu protokol otentikasi, yaitu ID pengguna, tidak diimplementasikan karena belum adanya proses otentikasi pengguna di dalamnya. Metrik kesesuaian aturan otentikasi mendapatkan nilai 0,375 pada pengujian pertama dikarenakan aturan-aturan otentikasi yang diperlukan sistem ini agar aman belum diimplementasikan seluruhnya.

Pengujian tahap kedua menunjukkan bahwa perubahan dan penambahan fitur yang diimplementasikan ke dalam sistem, berupa fitur-fitur yang berhubungan dengan kerahasiaan data dan otentisitas pengguna, memberikan dampak besar terhadap pengujian kedua metrik tersebut. Beberapa fitur merupakan fitur yang baru ditambahkan ke dalam sistem dan ada pula fitur yang menggantikan fitur yang sebelumnya sudah ada di dalam sistem. Selain itu, penambahan peran pengguna pada sistem baru juga memberikan dampak akan pengujian kerahasiaan data sistem dalam menyaring hak akses pengguna dalam penggunaan sistem. Daftar fitur yang diimplementasikan ke dalam sistem dan berhubungan dengan metrik pengujian pada Tugas Akhir ini diringkas pada Tabel 5.24 dan daftar peran pengguna dituliskan pada Tabel 5.25.

**Tabel 5.24. Ringkasan Modifikasi Sistem e-PKK Online**

<b>Nama Proses / Fitur</b>	<b>Sistem Lama</b>	<b>Sistem Baru</b>
Pengendalian hak akses	<i>Login</i> Registrasi	<i>Login</i> Registrasi Perangkat Tengah
Otentikasi pengguna web	<i>Sentinel 2.0</i>	Kelas <i>Auth Laravel</i>
Otentikasi pengguna perangkat bergerak	-	Token akun perangkat bergerak
Enkripsi & dekripsi data aplikasi web	Fungsi <i>hash</i> Sentinel	Fungsi hash <i>Auth Laravel</i>
Enkripsi & dekripsi data aplikasi perangkat bergerak	-	AES CryptoJS
Peran pengguna	-	Pengurus PKK Pengurus Posyandu Administrator
Kehilangan identitas	-	<i>Reset</i> kata sandi <i>Reset</i> token akun
Protokol otentikasi	Nama pengguna Nomor HP Kata Sandi	Nama pengguna Nomor HP Kata Sandi ID Pengguna
Aturan otentikasi	<i>Login</i> Ubah kata sandi	<i>Login</i> Registrasi Ubah kata sandi Perangkat tengah Verifikasi akun

**Tabel 5.25. Daftar Peran Pengguna Sistem e-PKK Online**

<b>Peran Pengguna</b>	<b>Hak Akses Halaman</b>	
Pengurus PKK	Keluhan anggota	Profil akun PKK
	Periode kepengurusan PKK	Jabatan kepengurusan PKK
	Pengurus PKK	Anggota PKK
	Kas PKK	Jenis kas PKK

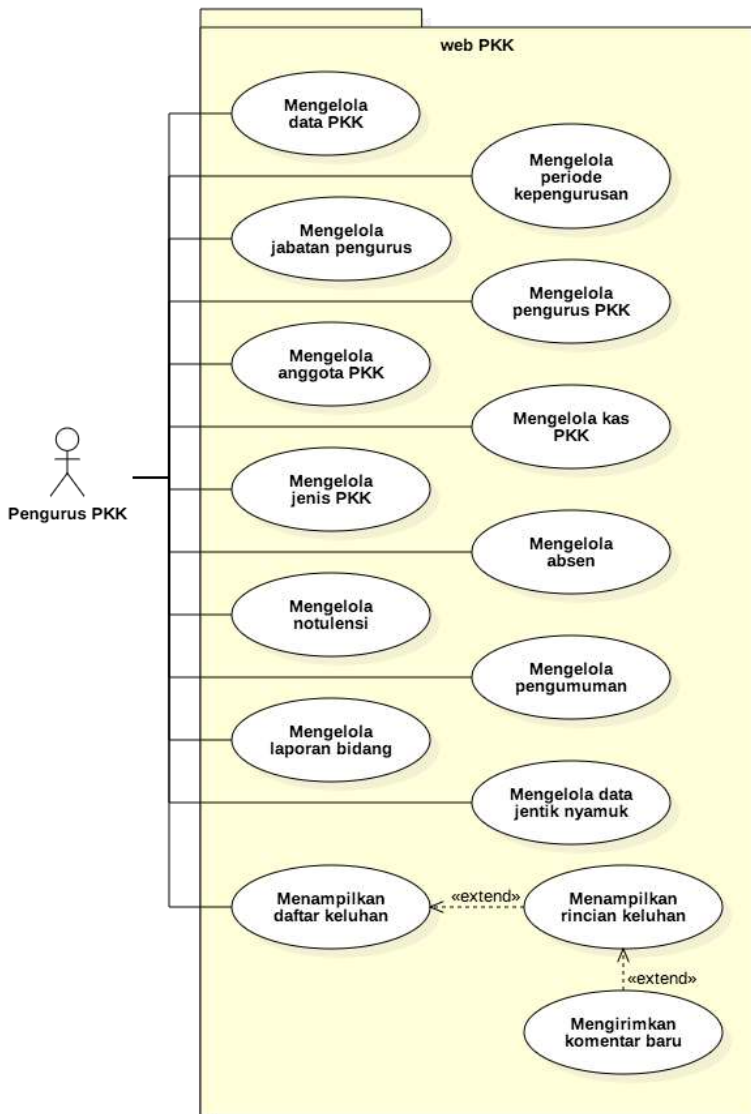
Peran Pengguna	Hak Akses Halaman	
	Kegiatan PKK	Absensi PKK
	Notulensi PKK	Pengumuman PKK
	Laporan bidang	Data jentik nyamuk
Pengurus Posyandu	Profil akun Posyandu	Data ibu Posyandu
	Data balita Posyandu	Pengurus Posyandu
	Kas Posyandu	Absen Posyandu
	Data penimbangan	Data imunisasi
	Data vitamin	Data keluhan anggota
Administrator PKK	Profil administrator	Manajemen akun pengguna PKK
Administrator Posyandu	Profil administrator	Data akun Posyandu
	Data master imunisasi	Data akun per wilayah

## LAMPIRAN A.1. Kebutuhan Sistem PKK *Online*

**Tabel 7.1. Kebutuhan Fungsional Aplikasi Web PKK**

<b>Kode</b>	<b>Deskripsi kebutuhan</b>
WPK-001	Pengurus PKK dapat login, masuk ke dalam sistem
WPK-002	Pengurus PKK dapat logout, keluar dari sistem
WPK-003	Pengurus PKK dapat mengelola data PKK
WPK-004	Pengurus PKK dapat menambahkan data PKK baru
WPK-005	Pengurus PKK dapat mengubah data PKK
WPK-006	Pengurus PKK dapat menghapus data PKK
WPK-007	Pengurus PKK dapat melihat rincian data PKK
WPK-008	Pengurus PKK dapat mengelola periode kepengurusan PKK
WPK-009	Pengurus PKK dapat menambahkan periode kepengurusan
WPK-010	Pengurus PKK dapat mengubah periode kepengurusan
WPK-011	Pengurus PKK dapat menghapus periode kepengurusan
WPK-012	Pengurus PKK dapat mengelola jabatan pengurus PKK
WPK-013	Pengurus PKK dapat menambahkan jabatan pengurus PKK
WPK-014	Pengurus PKK dapat mengubah jabatan pengurus PKK
WPK-015	Pengurus PKK dapat menghapus jabatan pengurus PKK
WPK-016	Pengurus PKK dapat mengelola pengurus PKK
WPK-017	Pengurus PKK dapat menambahkan pengurus PKK
WPK-018	Pengurus PKK dapat mengubah pengurus PKK
WPK-019	Pengurus PKK dapat menghapus pengurus PKK
WPK-020	Pengurus PKK dapat mengelola anggota/ibu PKK
WPK-021	Pengurus PKK dapat menambahkan anggota/ibu PKK
WPK-022	Pengurus PKK dapat mengubah anggota/ibu PKK
WPK-023	Pengurus PKK dapat menghapus anggota/ibu PKK
WPK-024	Pengurus PKK dapat melihat rincian anggota/ibu PKK
WPK-025	Pengurus PKK dapat mengelola kas PKK
WPK-026	Pengurus PKK dapat menambahkan kas PKK
WPK-027	Pengurus PKK dapat mengubah kas PKK
WPK-028	Pengurus PKK dapat menghapus kas PKK
WPK-029	Pengurus PKK dapat mengelola jenis kas PKK
WPK-030	Pengurus PKK dapat menambahkan jenis kas PKK
WPK-031	Pengurus PKK dapat mengubah jenis kas PKK
WPK-032	Pengurus PKK dapat menghapus jenis kas PKK
WPK-033	Pengurus PKK dapat mengelola absen PKK
WPK-034	Pengurus PKK dapat menambahkan absen PKK
WPK-035	Pengurus PKK dapat mengubah absen PKK

Kode	Deskripsi kebutuhan
WPK-036	Pengurus PKK dapat menghapus absen PKK
WPK-037	Pengurus PKK dapat mengelola notulensi PKK
WPK-038	Pengurus PKK dapat menambahkan notulensi PKK
WPK-039	Pengurus PKK dapat mengubah notulensi PKK
WPK-040	Pengurus PKK dapat menghapus notulensi PKK
WPK-041	Pengurus PKK dapat mengelola pengumuman PKK
WPK-042	Pengurus PKK dapat menambahkan pengumuman PKK
WPK-043	Pengurus PKK dapat mengubah pengumuman PKK
WPK-044	Pengurus PKK dapat menghapus pengumuman PKK
WPK-045	Pengurus PKK dapat melihat rincian pengumuman PKK
WPK-046	Pengurus PKK dapat mengelola laporan bidang PKK
WPK-047	Pengurus PKK dapat menambahkan laporan bidang PKK
WPK-048	Pengurus PKK dapat menghapus laporan bidang PKK
WPK-049	Pengurus PKK dapat mengunduh laporan bidang PKK
WPK-050	Pengurus PKK dapat mengelola data jentik nyamuk
WPK-051	Pengurus PKK dapat menambah data jentik nyamuk
WPK-052	Pengurus PKK dapat mengubah data jentik nyamuk
WPK-053	Pengurus PKK dapat menghapus data jentik nyamuk
WPK-054	Pengurus PKK dapat menampilkan daftar keluhan
WPK-055	Pengurus PKK dapat menampilkan rincian keluhan
WPK-056	Pengurus PKK dapat mengirimkan komentar pada suatu keluhan
WPK-057	Pengurus PKK dapat mengelola kegiatan PKK
WPK-058	Pengurus PKK dapat menambah kegiatan
WPK-059	Pengurus PKK dapat mengubah kegiatan
WPK-060	Pengurus PKK dapat menghapus kegiatan



**Gambar 7.1. Diagram Kasus Penggunaan Aplikasi Web PKK**

**Tabel 7.2. Deskripsi Diagram Kasus Penggunaan Aplikasi Web PKK**

<b>Kode</b>	<b>Nama</b>	<b>Keterangan</b>
UC-101	Mengelola data PKK	Pengguna dapat mengelola data PKK
UC-102	Tambah data PKK	Pengguna dapat menambahkan data PKK
UC-103	Ubah data PKK	Pengguna dapat mengubah data PKK
UC-104	Hapus data PKK	Pengguna dapat menghapus data PKK
UC-105	Tampilkan rincian data PKK	Pengguna dapat menampilkan rincian data PKK
UC-106	Mengelola periode kepengurusan	Pengguna dapat mengelola periode kepengurusan PKK
UC-107	Tambah periode	Pengguna dapat menambah periode
UC-108	Ubah periode	Pengguna dapat mengubah periode
UC-109	Hapus periode	Pengguna dapat menghapus periode
UC-110	Mengelola jabatan pengurus	Pengguna dapat mengelola jabatan pengurus PKK
UC-111	Tambah jabatan	Pengguna dapat menambah jabatan
UC-112	Ubah jabatan	Pengguna dapat mengubah jabatan
UC-113	Hapus jabatan	Pengguna dapat menghapus jabatan
UC-114	Mengelola pengurus PKK	Pengguna dapat mengelola pengurus PKK
UC-115	Tambah pengurus	Pengguna dapat menambah pengurus PKK
UC-116	Ubah pengurus	Pengguna dapat mengubah pengurus PKK
UC-117	Hapus pengurus	Pengguna dapat menghapus pengurus PKK
UC-118	Mengelola anggota PKK	Pengguna dapat mengelola anggota PKK
UC-119	Tambah anggota	Pengguna dapat menambah anggota PKK
UC-120	Ubah anggota	Pengguna dapat mengubah anggota PKK
UC-121	Hapus anggota	Pengguna dapat menghapus anggota PKK
UC-122	Tampilkan rincian anggota	Pengguna dapat menampilkan rincian anggota PKK
UC-123	Mengelola kas PKK	Pengguna dapat mengelola kas PKK



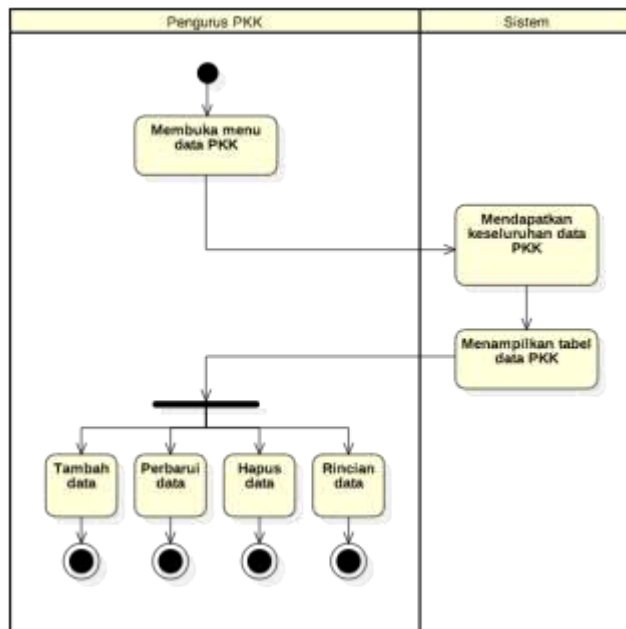
Kode	Nama	Keterangan
UC-124	Tambah kas	Pengguna dapat menambah kas PKK
UC-125	Ubah kas	Pengguna dapat mengubah kas PKK
UC-126	Hapus kas	Pengguna dapat menghapus kas PKK
UC-127	Mengelola jenis kas PKK	Pengguna dapat mengelola jenis kas PKK
UC-128	Tambah jenis kas	Pengguna dapat menambah jenis kas PKK
UC-129	Ubah jenis kas	Pengguna dapat mengubah jenis kas PKK
UC-130	Hapus jenis kas	Pengguna dapat menghapus jenis kas PKK
UC-131	Mengelola absen	Pengguna dapat mengelola absen PKK
UC-132	Tambah absen	Pengguna dapat menambah absen PKK
UC-133	Ubah absen	Pengguna dapat mengubah absen PKK
UC-134	Hapus absen	Pengguna dapat menghapus absen PKK
UC-135	Mengelola notulensi	Pengguna dapat mengelola notulensi PKK
UC-136	Tambah notulensi	Pengguna dapat menambah notulensi PKK
UC-137	Ubah notulensi	Pengguna dapat mengubah notulensi PKK
UC-138	Hapus notulensi	Pengguna dapat menghapus notulensi PKK
UC-139	Mengelola pengumuman	Pengguna dapat mengelola pengumuman PKK
UC-140	Tambah pengumuman	Pengguna dapat menambah pengumuman PKK
UC-141	Ubah pengumuman	Pengguna dapat mengubah pengumuman PKK
UC-142	Hapus pengumuman	Pengguna dapat menghapus pengumuman PKK
UC-143	Melihat rincian pengumuman	Pengguna dapat melihat rincian pengumuman PKK
UC-144	Mengelola laporan bidang	Pengguna dapat mengelola laporan bidang PKK
UC-145	Tambah laporan bidang	Pengguna dapat menambah laporan bidang PKK

Kode	Nama	Keterangan
UC-146	Hapus laporan bidang	Pengguna dapat menghapus laporan bidang PKK
UC-147	Unduh laporan bidang	Pengguna dapat mengunduh laporan bidang PKK
UC-148	Mengelola data jentik nyamuk	Pengguna dapat mengelola data jentik nyamuk
UC-149	Tambah data jentik	Pengguna dapat menambah data jentik nyamuk
UC-150	Ubah data jentik	Pengguna dapat mengubah data jentik nyamuk
UC-151	Hapus data jentik	Pengguna dapat menghapus data jentik nyamuk
UC-152	Menampilkan daftar keluhan	Pengguna dapat menampilkan daftar keluhan
UC-153	Menampilkan rincian keluhan	Pengguna dapat menampilkan rincian suatu keluhan tertentu
UC-154	Mengirimkan komentar baru	Pengguna dapat mengirimkan komentar baru pada suatu keluhan
UC-155	Mengelola kegiatan PKK	Pengguna dapat mengelola kegiatan PKK
UC-156	Tambah kegiatan	Pengguna dapat menambah kegiatan PKK
UC-157	Ubah kegiatan	Pengguna dapat mengubah kegiatan PKK
UC-158	Hapus kegiatan	Pengguna data menghapus kegiatan PKK

**Tabel 7.3. Spesifikasi Kasus Penggunaan: Mengelola Data PKK**

Kode Use Case	UC-101
Nama Use Case	Mengelola data PKK
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola data PKK
Kondisi Awal	Pengurus PKK membuka menu data PKK
Kondisi Akhir	Pengurus PKK dapat mengelola data PKK: tambah, ubah, hapus, dan tampilkan rincian (UC-102-105)
Alur Kejadian Normal	
Aktor	Sistem

1. Pengurus PKK membuka menu data PKK  4. Pengurus PKK dapat melakukan: 4A. Tambah data PKK (UC-102) 4B. Ubah data PKK (UC-103) 4C. Hapus data PKK (UC-104) 4D. Tampilkan rincian data PKK (UC-105)	2. Sistem mendapatkan data PKK 3. Sistem menampilkan tabel data PKK
---	--

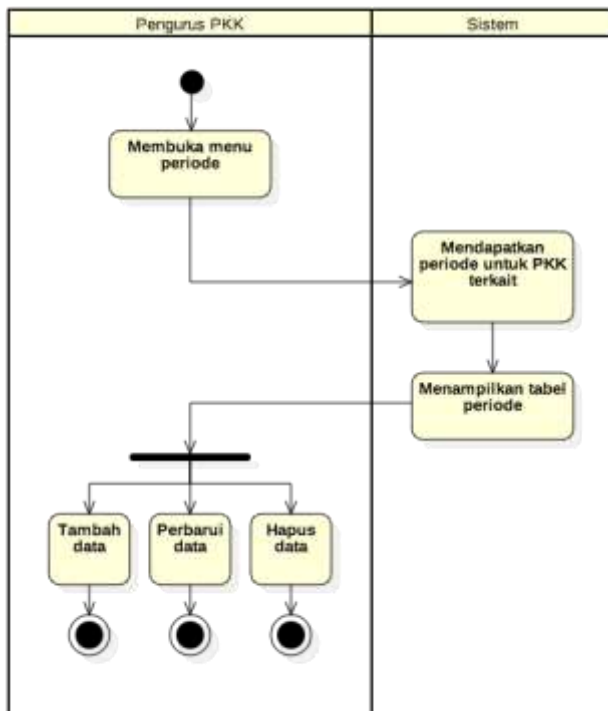


**Gambar 7.2. Diagram Aktivitas: Mengelola Data PKK**

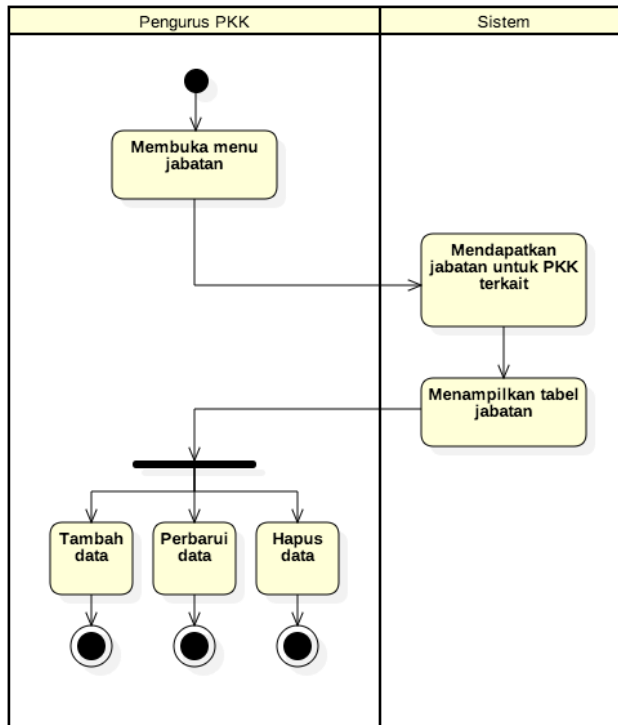
**Tabel 7.4. Spesifikasi Kasus Penggunaan: Mengelola Periode Kepengurusan**

Kode Use Case	UC-106
Nama Use Case	Mengelola periode kepengurusan
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola periode kepengurusan

Kondisi Awal	Pengurus PKK membuka menu periode
Kondisi Akhir	Pengurus PKK dapat mengelola periode kepengurusan: tambah, ubah, dan hapus (UC-107-109)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu periode  4. Pengurus PKK dapat melakukan: 4A. Tambah periode (UC-107) 4B. Ubah periode (UC-108) 4C. Hapus periode (UC-109)	2. Sistem mendapatkan periode kepengurusan untuk PKK terkait 3. Sistem menampilkan tabel berisi periode kepengurusan



**Gambar 7.3. Diagram Aktivitas: Mengelola Periode Kepengurusan**

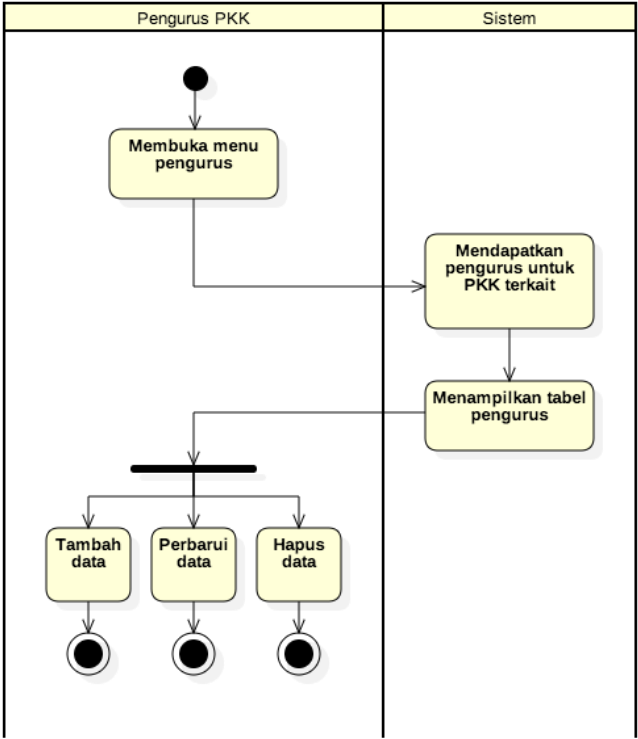


**Gambar 7.4. Diagram Aktivitas: Mengelola Jabatan Pengurus**

**Tabel 7.5. Spesifikasi Kasus Penggunaan: Mengelola Jabatan Pengurus**

Kode Use Case	UC-110
Nama Use Case	Mengelola jabatan pengurus
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola jabatan pengurus
Kondisi Awal	Pengurus PKK membuka menu jabatan
Kondisi Akhir	Pengurus PKK dapat mengelola jabatan pengurus: tambah, ubah, dan hapus (UC-111-113)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu jabatan	2. Sistem mendapatkan jabatan pengurus untuk PKK terkait

4. Pengurus PKK dapat melakukan berbagai aksi 4A. Tambah jabatan (UC-111) 4B. Ubah jabatan (UC-112) 4C. Hapus jabatan (UC-113)	3. Sistem menampilkan tabel berisi jabatan pengurus
---	---



Gambar 7.5. Diagram Aktivitas: Mengelola Pengurus PKK

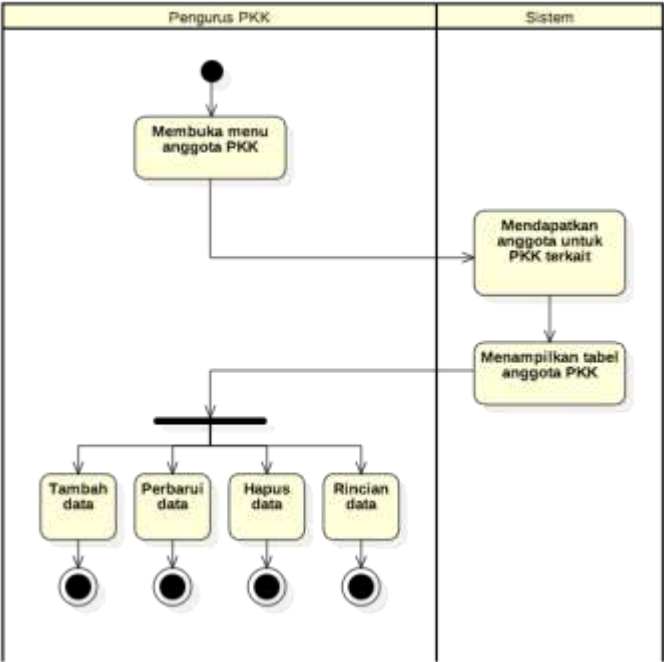
Tabel 7.6. Spesifikasi Kasus Penggunaan: Mengelola Pengurus PKK

Kode Use Case	UC-114
Nama Use Case	Mengelola pengurus PKK
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola pengurus PKK

Kondisi Awal	Pengurus PKK membuka menu pengurus
Kondisi Akhir	Pengurus PKK dapat mengelola pengurus PKK: tambah, ubah, dan hapus (UC-115-117)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu pengurus        4. Pengurus PKK dapat melakukan berbagai aksi 4A. Tambah pengurus (UC-115) 4B. Ubah pengurus (UC-116) 4C. Hapus pengurus (UC-117)	2. Sistem mendapatkan pengurus untuk PKK terkait 3. Sistem menampilkan tabel berisi pengurus PKK

**Tabel 7.7. Spesifikasi Kasus Penggunaan: Mengelola Anggota PKK**

Kode Use Case	UC-118
Nama Use Case	Mengelola anggota PKK
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola anggota PKK
Kondisi Awal	Pengurus PKK membuka menu anggota
Kondisi Akhir	Pengurus PKK dapat mengelola anggota PKK: tambah, ubah, hapus, dan tampilkan rincian (UC-119-122)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu anggota        4. Pengurus PKK dapat melakukan berbagai aksi 4A. Tambah anggota PKK (UC-119) 4B. Ubah anggota PKK (UC-120) 4C. Hapus anggota PKK (UC-121) 4D. Tampilkan rincian anggota PKK (UC-122)	2. Sistem mendapatkan anggota untuk PKK terkait 3. Sistem menampilkan tabel berisi anggota PKK



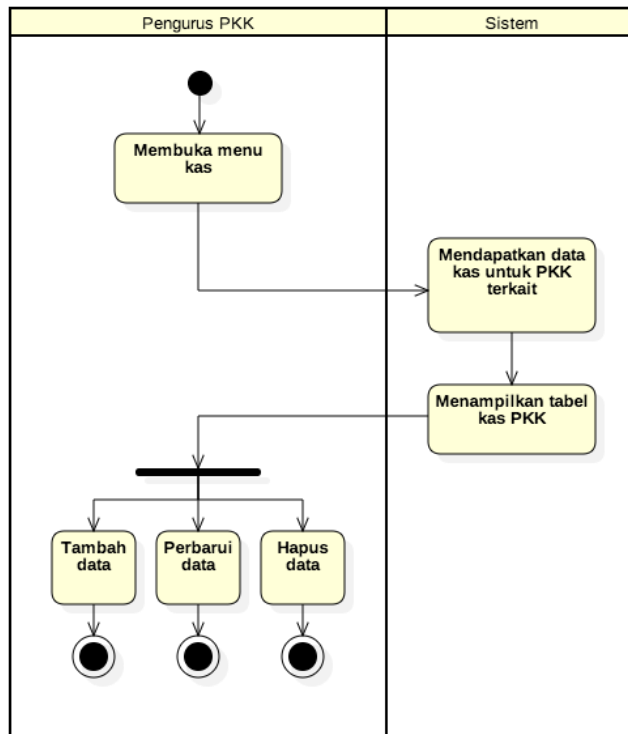
Gambar 7.6. Diagram Aktivitas: Mengelola Anggota PKK

Tabel 7.8. Spesifikasi Kasus Penggunaan: Mengelola Kas PKK

Kode Use Case	UC-123
Nama Use Case	Mengelola kas PKK
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola kas PKK
Kondisi Awal	Pengurus PKK membuka menu kas
Kondisi Akhir	Pengurus PKK dapat mengelola kas PKK: tambah, ubah, dan hapus (UC-124-126)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu kas	2. Sistem mendapatkan kas untuk PKK terkait 3. Sistem menampilkan tabel berisi kas PKK



4. Pengurus PKK dapat melakukan berbagai aksi 4A. Tambah kas (UC-124) 4B. Ubah kas (UC-125) 4C. Hapus kas (UC-126)	
---	--

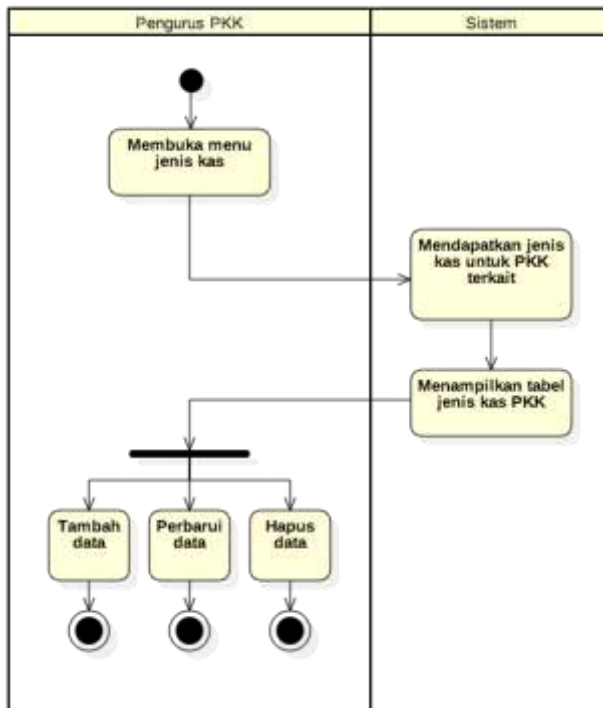


**Gambar 7.7. Diagram Aktivitas: Mengelola Kas PKK**

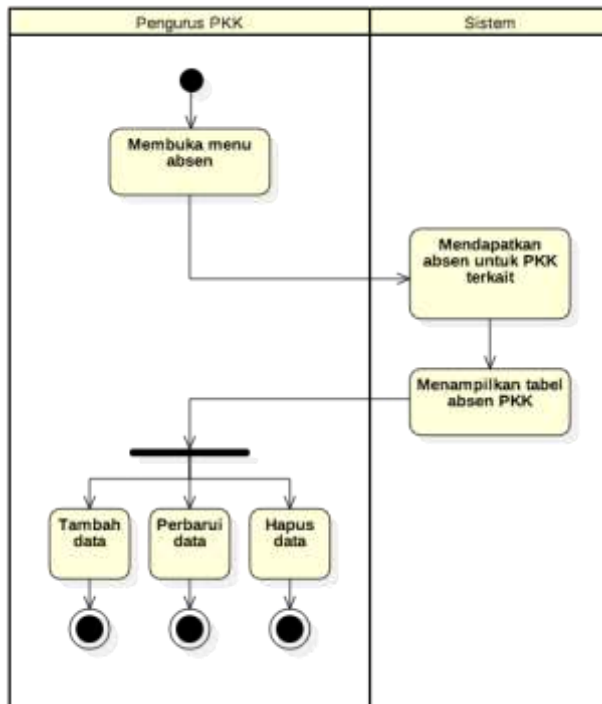
**Tabel 7.9. Spesifikasi Kasus Penggunaan: Mengelola Jenis Kas PKK**

Kode Use Case	UC-127
Nama Use Case	Mengelola jenis kas PKK
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola jenis kas PKK
Kondisi Awal	Pengurus PKK membuka menu jenis kas

Kondisi Akhir	Pengurus PKK dapat mengelola jenis kas PKK: tambah, ubah, dan hapus (UC-128-130)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu jenis kas          4. Pengurus PKK dapat melakukan berbagai aksi 4A. Tambah jenis kas (UC-128) 4B. Ubah jenis kas (UC-129) 4C. Hapus jenis kas (UC-130)	2. Sistem mendapatkan jenis kas untuk PKK terkait 3. Sistem menampilkan tabel berisi jenis kas PKK



**Gambar 7.8. Diagram Aktivitas: Mengelola Jenis Kas PKK**

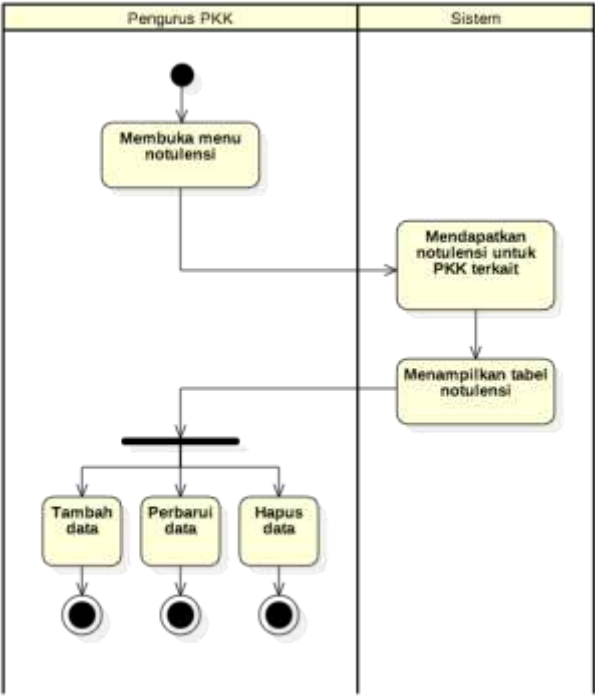


**Gambar 7.9. Diagram Aktivitas: Mengelola Absen**

**Tabel 7.10. Spesifikasi Kasus Penggunaan: Mengelola Absen**

Kode Use Case	UC-131
Nama Use Case	Mengelola absen
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola absen
Kondisi Awal	Pengurus PKK membuka menu absen
Kondisi Akhir	Pengurus PKK dapat mengelola absen: tambah, ubah, dan hapus (UC-132-134)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu absen	2. Sistem mendapatkan absen untuk PKK terkait

4. Pengurus PKK dapat melakukan berbagai aksi 4A. Tambah absen (UC-132) 4B. Ubah absen (UC-133) 4C. Hapus absen (UC-134)	3. Sistem menampilkan tabel berisi absen PKK
---	--



Gambar 7.10. Diagram Aktivitas: Mengelola Notulensi

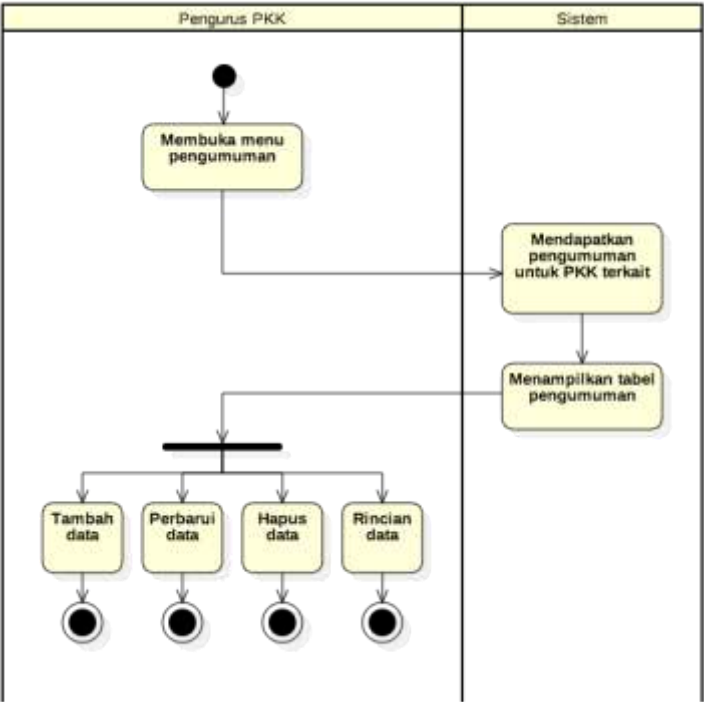
Tabel 7.11. Spesifikasi Kasus Penggunaan: Mengelola Notulensi

Kode Use Case	UC-135
Nama Use Case	Mengelola notulensi
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola notulensi
Kondisi Awal	Pengurus PKK membuka menu notulensi

Kondisi Akhir	Pengurus PKK dapat mengelola notulensi: tambah, ubah, dan hapus (UC-136-138)	
Alur Kejadian Normal		
Aktor		Sistem
1. Pengurus PKK membuka menu notulensi		2. Sistem mendapatkan notulensi untuk PKK terkait 3. Sistem menampilkan tabel berisi notulensi PKK
4. Pengurus PKK dapat melakukan berbagai aksi		
4A. Tambah notulensi (UC-136)		
4B. Ubah notulensi (UC-137)		
4C. Hapus notulensi (UC-138)		

**Tabel 7.12. Spesifikasi Kasus Penggunaan: Mengelola Pengumuman**

Kode Use Case	UC-139
Nama Use Case	Mengelola pengumuman
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola pengumuman
Kondisi Awal	Pengurus PKK membuka menu pengumuman
Kondisi Akhir	Pengurus PKK dapat mengelola pengumuman: tambah, ubah, hapus, dan tampilkan rincian (UC-140-143)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu pengumuman	2. Sistem mendapatkan pengumuman untuk PKK terkait
	3. Sistem menampilkan tabel berisi pengumuman
4. Pengurus PKK dapat melakukan berbagai aksi	
4A. Tambah pengumuman (UC-140)	
4B. Ubah pengumuman (UC-141)	
4C. Hapus pengumuman (UC-142)	
4D. Tampilkan rincian pengumuman (UC-143)	

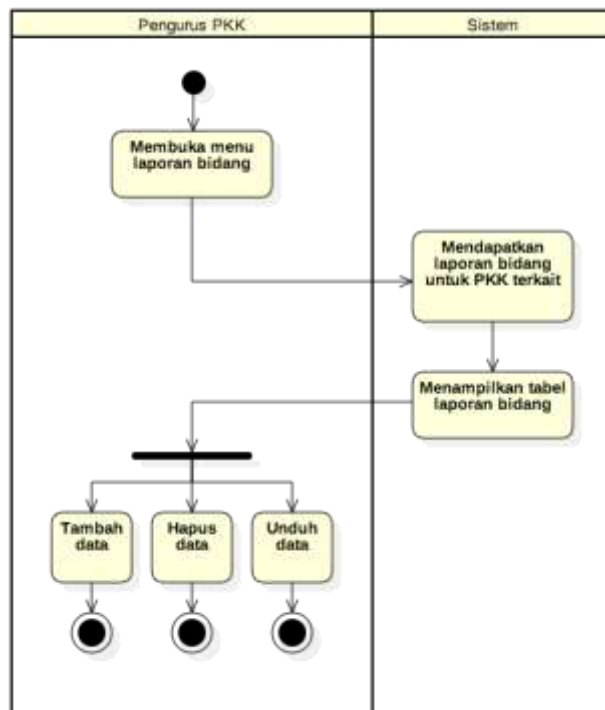


Gambar 7.11. Diagram Aktivitas: Mengelola Pengumuman

Tabel 7.13. Spesifikasi Kasus Penggunaan: Mengelola Laporan Bidang

Kode Use Case	UC-144	
Nama Use Case	Mengelola laporan bidang	
Aktor	Pengurus PKK	
Deskripsi	Pengurus PKK dapat mengelola laporan bidang	
Kondisi Awal	Pengurus PKK membuka menu laporan bidang	
Kondisi Akhir	Pengurus PKK dapat mengelola laporan bidang: tambah, hapus, dan unduh (UC-145-147)	
Alur Kejadian Normal		
Aktor		Sistem
1. Pengurus PKK membuka menu laporan bidang		2. Sistem mendapatkan laporan bidang untuk PKK terkait

<p>4. Pengurus PKK dapat melakukan berbagai aksi</p> <p>4A. Tambah laporan bidang (UC-145)</p> <p>4B. Hapus laporan bidang (UC-146)</p> <p>4C. Unduh laporan bidang (UC-147)</p>	<p>3. Sistem menampilkan tabel berisi daftar laporan bidang</p>
--	---

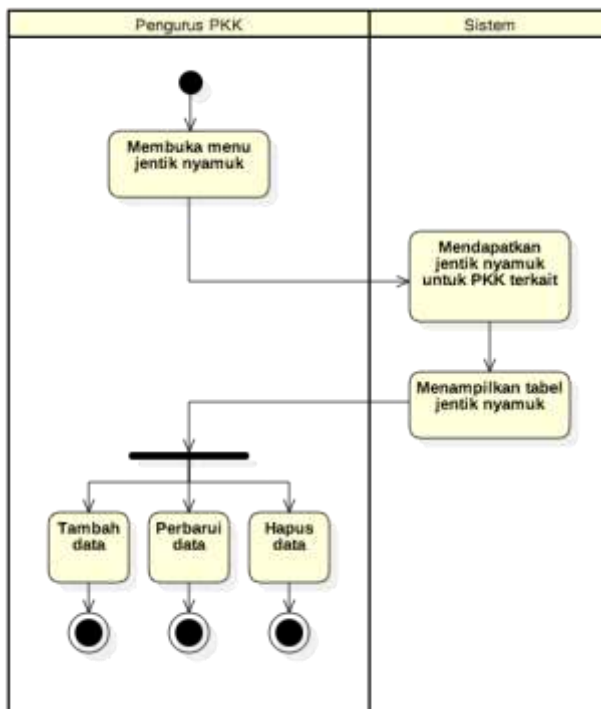


**Gambar 7.12. Diagram Aktivitas: Mengelola Laporan Bidang**

**Tabel 7.14. Spesifikasi Kasus Penggunaan: Mengelola Data Jentik Nyamuk**

Kode Use Case	UC-148
Nama Use Case	Mengelola data jentik nyamuk
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengelola data jentik nyamuk
Kondisi Awal	Pengurus PKK membuka menu jentik

Kondisi Akhir	Pengurus PKK dapat mengelola data jentik nyamuk: tambah, ubah, dan hapus (UC-149-151)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu jentik       4. Pengurus PKK dapat melakukan berbagai aksi 4A. Tambah data jentik (UC-149) 4B. Ubah data jentik (UC-150) 4C. Hapus data jentik (UC-151)	2. Sistem mendapatkan data jentik nyamuk untuk PKK terkait 3. Sistem menampilkan tabel berisi data jentik nyamuk

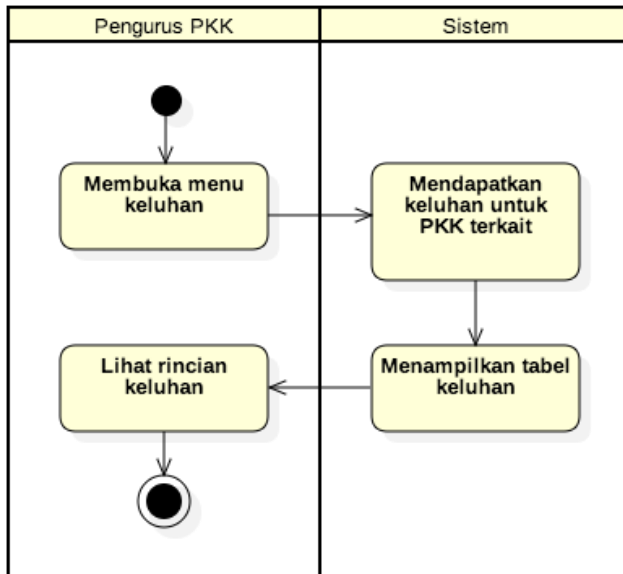


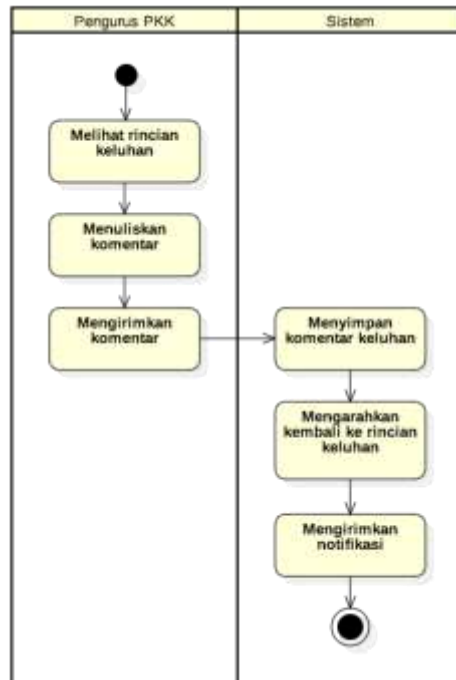
**Gambar 7.13. Diagram Aktivitas: Mengelola Data Jentik Nyamuk**



**Tabel 7.15. Spesifikasi Kasus Penggunaan: Menampilkan Daftar Keluhan**

Kode Use Case	UC-152
Nama Use Case	Menampilkan daftar keluhan
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat menampilkan daftar keluhan
Kondisi Awal	Pengurus PKK membuka menu keluhan
Kondisi Akhir	Pengurus PKK dapat melihat keluhan-keluhan yang dikirimkan anggota PKK dan dapat melihat rincian keluhan (UC-153)
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK membuka menu keluhan	2. Sistem mendapatkan keluhan untuk PKK terkait 3. Sistem menampilkan tabel berisi keluhan
4. Pengurus PKK dapat melihat rincian keluhan (UC-153)	

**Gambar 7.14. Diagram Aktivitas: Menampilkan Daftar Keluhan**



**Gambar 7.15. Diagram Aktivitas: Mengirimkan Komentar Baru**

**Tabel 7.16. Spesifikasi Kasus Penggunaan: Mengirimkan Komentar Baru**

Kode Use Case	UC-154
Nama Use Case	Mengirimkan komentar baru
Aktor	Pengurus PKK
Deskripsi	Pengurus PKK dapat mengirimkan komentar baru pada suatu keluhan
Kondisi Awal	Pengurus PKK membuka melihat rincian sebuah keluhan
Kondisi Akhir	Komentar baru pengurus PKK pada sebuah keluhan disimpan di dalam sistem
Alur Kejadian Normal	
Aktor	Sistem
1. Pengurus PKK melihat rincian keluhan	

2. Pengurus PKK menuliskan komentar pada kolom yang disediakan	
3. Pengurus PKK menekan tombol simpan	4. Sistem menyimpan komentar keluhan 5. Sistem mengarahkan kembali ke rincian keluhan dan mengirimkan notifikasi berhasil

**Tabel 7.17. Fitur Aplikasi Ensiklopedia Kesehatan Balita dan Ibu Hamil**

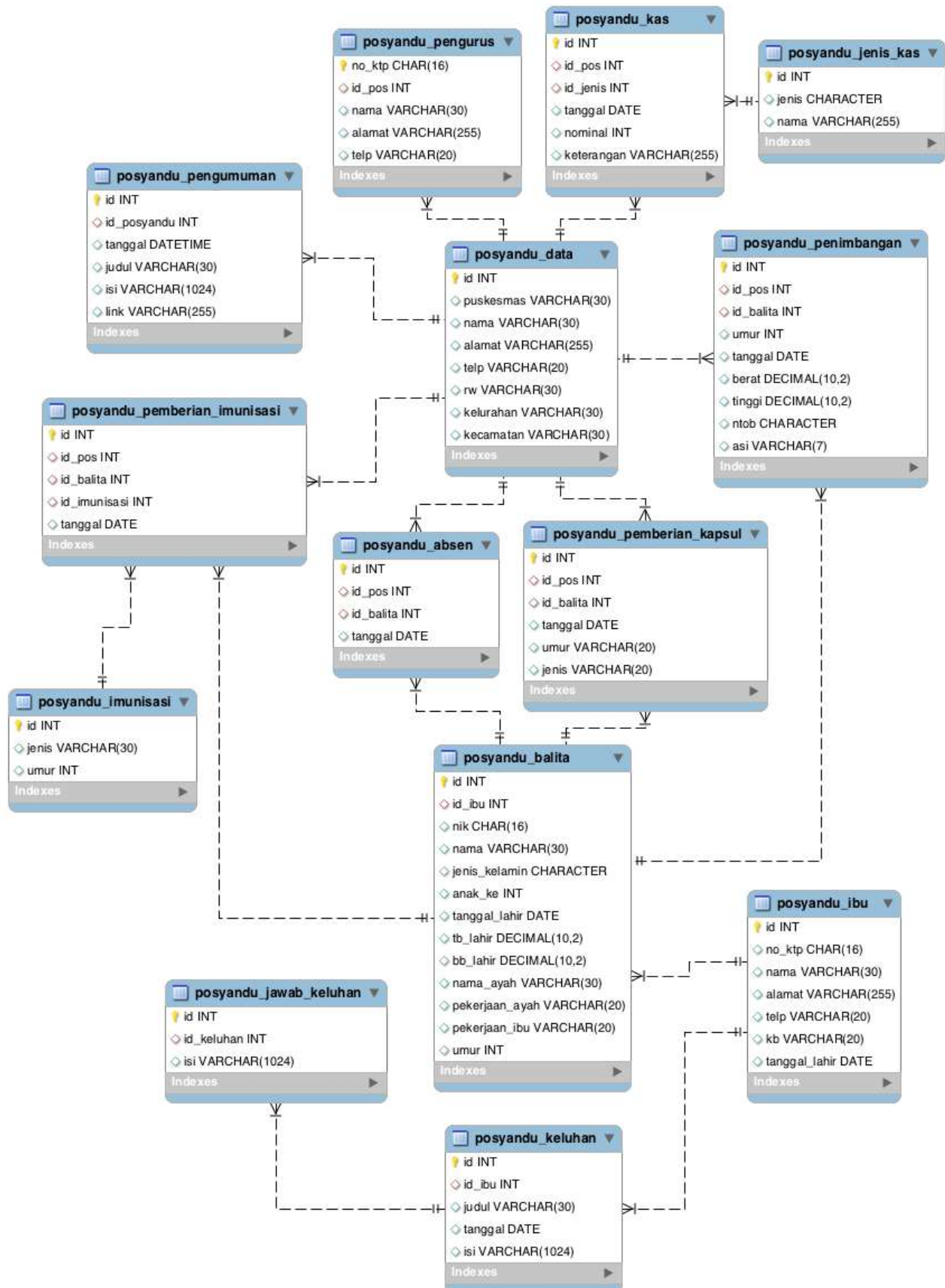
Kode	Fitur
ENS-003	Melihat informasi perkembangan kehamilan
ENS-004	Melihat rekomendasi olahraga untuk ibu hamil
ENS-005	Melihat rekomendasi pemeriksaan bagi ibu hamil
ENS-006	Melihat tips selama masa kehamilan
ENS-007	Melihat informasi persiapan kehamilan
ENS-008	Melihat tips persiapan kehamilan
ENS-009	Membaca FAQ ( <i>Frequently Asked Question</i> )

**Tabel 7.18. Kebutuhan Non-Fungsional Sistem e-PKK Online**

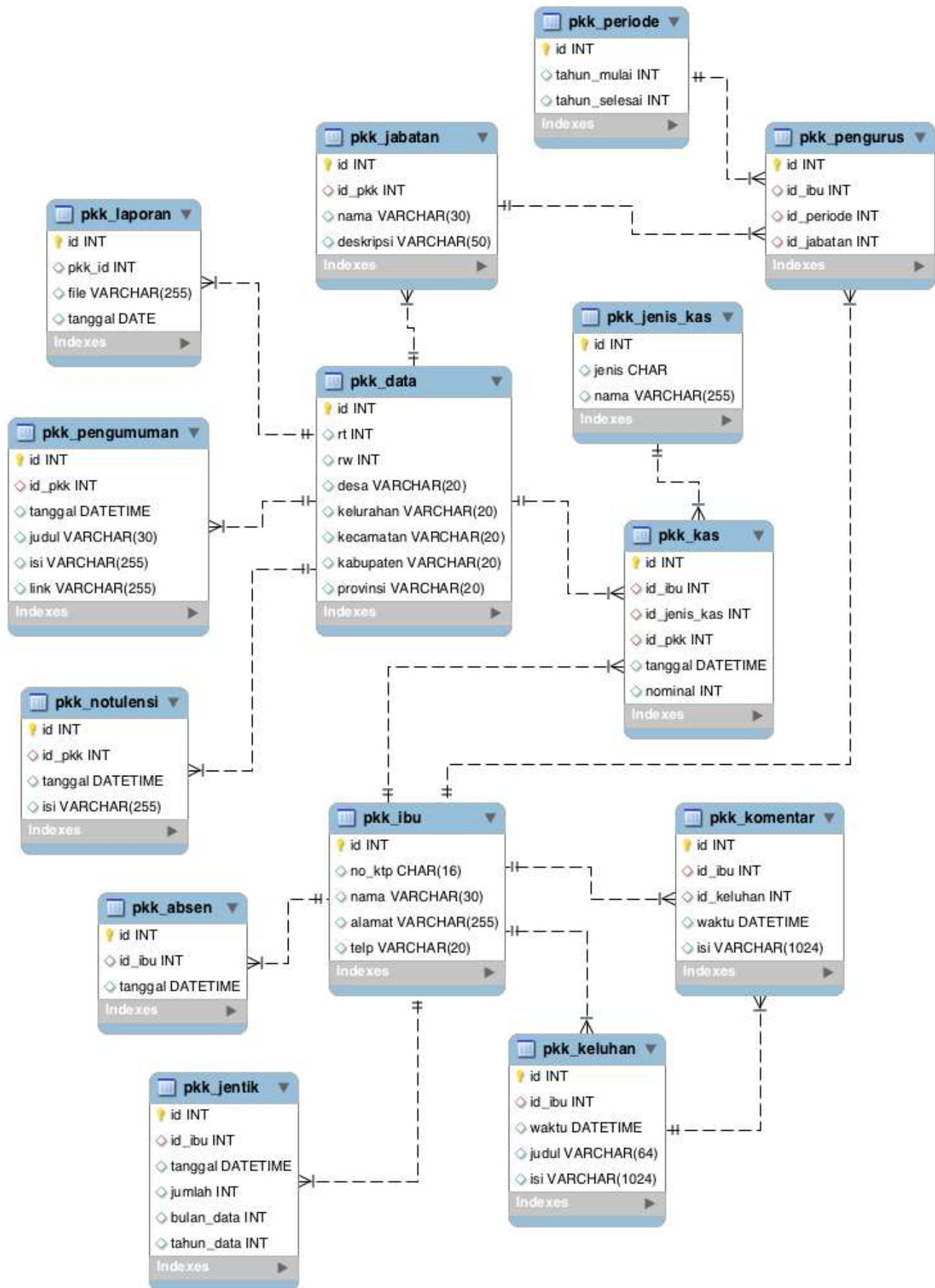
Kode	Deskripsi kebutuhan
NFR-001	Waktu maksimal <i>response time</i> adalah 4 detik
NFR-002	Sistem beroperasi 7 hari perminggu, 24 jam perhari
NFR-003	Data selalu tersedia dan ada <i>backup data</i>
NFR-004	Sistem memiliki <i>error handling</i> yang <i>user friendly</i>
NFR-005	Tampilan aplikasi <i>user friendly</i>
NFR-006	Format menu <i>user friendly</i>
NFR-007	Warna konsisten
NFR-008	Jenis <i>font</i> konsisten dan mudah dibaca
NFR-009	Sistem menggunakan Bahasa Indonesia

*[Halaman ini sengaja dikosongkan]*

## LAMPIRAN A.2. Basis Data Sistem e-PKK Online



Gambar 8.1. PDM Sistem Posyandu



Gambar 8.2. PDM Sistem PKK

## **BAB VI**

### **KESIMPULAN DAN SARAN**

Pada bab ini diberikan kesimpulan yang diambil selama pengerjaan Tugas Akhir. Selain itu, diberikan pula saran-saran tentang pengembangan yang dapat dilakukan terhadap sistem yang dikembangkan pada Tugas Akhir ini di masa yang akan datang.

#### **6.1. Kesimpulan**

Kesimpulan yang diperoleh berdasarkan uji coba dan evaluasi yang telah dilakukan pada Tugas Akhir antara lain:

1. Sistem e-PKK *online* yang sudah ada belum memenuhi standar kerahasiaan data dan otentisitas pengguna menurut ISO 25010, dibuktikan dengan nilai yang didapatkan dari hasil pengujian tahap pertama pada Tugas Akhir ini. Hal ini disebabkan banyaknya kebutuhan mengenai penjagaan kerahasiaan data dan kebutuhan mengenali pengguna yang belum diimplementasikan ke dalam sistem.
2. Sistem e-PKK *online* yang sudah disesuaikan dengan standar kerahasiaan data dan otentisitas pengguna menurut ISO 25010 dinilai sudah memenuhi standar, dibuktikan dengan nilai yang didapatkan dari hasil pengujian tahap kedua pada Tugas Akhir ini. Hal ini menandakan bahwa perubahan atau penambahan fitur dan kebutuhan dapat meningkatkan kualitas sistem sesuai dengan metrik yang diujikan.
3. Beberapa fitur yang dapat ditambahkan dalam rangka meningkatkan nilai pengujian kerahasiaan data dan otentisitas pengguna antara lain: pengaturan hak akses, penggunaan perangkat tengah, penggunaan algoritma kriptografi antar bahasa pemrograman, penjagaan kerahasiaan informasi penting pengguna, dan verifikasi akun pengguna.

## 6.2. Saran

Terdapat beberapa saran terkait Tugas Akhir ini yang diharapkan bisa membuat Tugas Akhir ini menjadi lebih baik. Saran-saran tersebut antara lain:

1. Beberapa fitur yang dapat ditambahkan sesuai dengan masukan dari responden kuisioner, antara lain: penambahan tingkat wilayah hingga tingkat Dasa Wisma, penambahan fitur TOGA (Tanaman Obat Keluarga), berita mengenai kegiatan PKK daerah lain.
2. Meskipun penilaian kemudahan aplikasi pada bagian tampilan sudah tinggi, rancangan dan tampilan aplikasi disarankan untuk lebih menarik karena responden merasa kurang adanya banyak gambar dan situs terlalu formal.
3. Perlu adanya fitur yang dapat membantu pengurus untuk membuat laporan dalam bentuk file dengan format tertentu, seperti PDF, agar keluaran sistem lebih berguna dan dapat diolah kembali.
4. Perlu adanya penyuluhan dan pengambilan sampel responden lebih banyak lagi karena budaya di tiap wilayah Indonesia berbeda dan tidak semuanya mengerti mengenai perkembangan teknologi layaknya masyarakat yang berada di wilayah kota dan mudah menjangkau internet.



## DAFTAR PUSTAKA

- [1] M. D. N. R. Indonesia, "Pedoman Pemberdayaan dan Kesejahteraan Keluarga dalam Membantu Meningkatkan dan Mewujudkan Tertib Administrasi Kependudukan". Indonesia Patent Peraturan Menteri Dalam Negeri Nomor 28 Tahun 2011, 7 July 2011.
- [2] Sekretariat TP PKK Pusat, "Pembinaan 10 Program Pokok PKK," Pemberdayaan dan Kesejahteraan Keluarga, 2015. [Online]. Available: <http://tp-pkkpusat.org/index.php>. [Accessed 31 May 2016].
- [3] M. D. N. R. Indonesia, "Pedoman Pengintegrasian Layanan Sosial Dasar di Pos Pelayanan Terpadu". Indonesia Patent Peraturan Menteri Dalam Negeri Nomor 19 Tahun 2011, 12 May 2011.
- [4] Pemda Cilacap, "Posyandu Indonesia," 2011. [Online]. Available: <http://posyandu.org/>. [Accessed 31 May 2016].
- [5] K. D. Dalmi, Rancang Bangun Aplikasi Perangkat Bergerak Sebagai Panduan Perkembangan dan Pemberian Nutrisi untuk Bayi Usia 0-2 Tahun, Surabaya: RBTC ITS, 2014.
- [6] ISO/IEC, ISO/IEC 25010:2015 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models, 2015.
- [7] "ISO 25000 PORTAL," 15 Desember 2015. [Online]. Available: <http://iso25000.com/index.php/en/iso-25000-standards>. [Accessed 2016 May 31].
- [8] TechTarget, "Search Security," TechTarget, [Online]. Available: <http://searchsecurity.techtarget.com/definition/authentication>. [Accessed 31 May 2016].

- [9] "Special Topics: Authentication and Authorization," Yii Software LLC., [Online]. Available: [www.yiiframework.com/doc/guide/1.1/en/topics.auth](http://www.yiiframework.com/doc/guide/1.1/en/topics.auth). [Accessed 31 May 2016].
- [10] T. Otwell, "Laravel - The PHP Framework For Web Artisan," June 2011. [Online]. Available: <https://laravel.com/>. [Accessed 31 May 2016].
- [11] Adobe, "PhoneGap," Apache, [Online]. Available: <http://phonegap.com/>. [Accessed 31 May 2016].
- [12] A. R. Soedjono, Rancang Bangun Aplikasi Panduan Informasi PKK pada Perangkat Bergerak, Surabaya: RBTC ITS, 2015.
- [13] F. Y. Sianipar, Pengujian Integritas Data Sistem Posyandu Online Menggunakan ISO 25010, Surabaya: RBTC ITS, 2016.
- [14] Cartalyst, "Sentinel Manual :: Cartalyst," Cartalyst LLC, 24 February 2015. [Online]. Available: <https://cartalyst.com/manual/sentinel/2.0>. [Accessed 31 May 2016].
- [15] W. Stallings, Cryptography and Network Security, Principles and Practice, Fifth Edition, New York: Pearson Education, Inc., 2011.
- [16] D. Crockford, "JSON," [Online]. Available: <http://www.json.org>. [Accessed 31 May 2016].

## BIODATA PENULIS



Penulis lahir di Surabaya, 24 Februari 1994. Penulis telah menempuh pendidikan dasar di SD Muhammadiyah IV Pucang, kemudian untuk pendidikan menengah pertama di SMPN 6 Surabaya dan di jenjang menengah atas di SMAN 1 Surabaya. Sejak kecil, penulis memiliki ketertarikan pada bidang komputer sehingga

penulis memutuskan untuk mengambil pendidikan sarjana S1 di Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya. Selama masa perkuliahan, penulis juga berorganisasi menjadi staf Departemen Kesejahteraan Mahasiswa Himpunan Mahasiswa Teknik Computer-Informatika (HMTIC) ITS 2013/2014, staf Departemen Pengembangan Sumber Daya Mahasiswa Pengurus UKM PSM ITS 2013/2014, Ketua UKM PSM ITS 2014/2015, dan Kepala Departemen Hubungan Masyarakat Lembaga Minat Bakat (LMB) ITS 2015/2016.

Penulis dalam menyelesaikan pendidikan S1 mengambil rumpun mata kuliah (RMK) Rekayasa Perangkat Lunak serta memiliki ketertarikan di bidang Manajemen Proyek Perangkat Lunak, Pemrograman *Web* dan *Mobile*, Penjaminan Kualitas Perangkat Lunak, dan *Big Data*. Untuk komunikasi, penulis dapat dihubungi melalui alamat email: [arsoedjono@gmail.com](mailto:arsoedjono@gmail.com).

*[Halaman ini sengaja dikosongkan]*